AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

FEDERAL REGISTER

Vol. 79 Thursday,
No. 176 September 11, 2014

Part VI

Department of the Treasury

Office of the Comptroller of the Currency

12 CFR Parts 30, 168, and 170
OCC Guidelines Establishing Heightened Standards for Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches; Integration of Regulations; Final Rule

DEPARTMENT OF THE TREASURY

Office of the Comptroller of the Currency

12 CFR Parts 30, 168, and 170

[Docket ID OCC–2014–001]

RIN 1557–AD78

OCC Guidelines Establishing Heightened Standards for Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches; Integration of Regulations

AGENCY: Office of the Comptroller of the Currency, Treasury.

ACTION: Final rules and guidelines.

SUMMARY: The Office of the Comptroller of the Currency (OCC) is adopting guidelines, issued as an appendix to its safety and soundness standards regulations, establishing minimum standards for the design and implementation of a risk governance framework (Framework) for large insured national banks, insured Federal savings associations, and insured Federal branches of foreign banks (banks) with average total consolidated assets of $50 billion or more and minimum standards for a board of directors in overseeing the Framework's design and implementation (final Guidelines). The standards contained in the final Guidelines will be enforceable by the terms of a Federal statute that authorizes the OCC to prescribe operational and managerial standards for national banks and Federal savings associations. In addition, as part of our ongoing efforts to integrate the regulations of the OCC and those of the Office of Thrift Supervision (OTS), the OCC is adopting final rules and guidelines that make its safety and soundness standards regulations and guidelines applicable to both national banks and Federal savings associations and that remove the comparable Federal savings association regulations and guidelines. The OCC is also adopting other technical changes to the safety and soundness standards regulations and guidelines.

DATES: The final rule is effective November 10, 2014. Compliance dates for the final Guidelines vary as specified.

FOR FURTHER INFORMATION CONTACT: Molly Scherf, Deputy Comptroller, Large Bank Supervision, (202) 649–6210, or Stuart Feldstein, Director, Andra Shuster, Senior Counsel, or Henry Barkhausen, Attorney, Legislative & Regulatory Activities Division, (202) 649–5490, for persons who are deaf or hard of hearing, TTY, (202) 649–5597, or Martin Chavez, Attorney, Securities and Corporate Practices Division, (202) 649–5510, 400 7th Street SW., Washington, DC 20219.

SUPPLEMENTARY INFORMATION:

Background

The recent financial crisis demonstrated the destabilizing effect that large, interconnected financial companies can have on the national economy, capital markets, and the overall financial stability of the banking system. The financial crisis and the accompanying legislative response underscore the importance of strong bank supervision and regulation of the financial system. Congress passed the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 (Dodd-Frank Act) [1] to address, in part, weaknesses in the framework for the supervision and regulation of large U.S. financial companies.[2] These legislative developments highlight the view that large, complex institutions can have a significant impact on capital markets and the economy and, therefore, need to be supervised and regulated more rigorously.

As a result of the financial crisis, the OCC developed a set of ''heightened expectations'' to enhance our supervision and strengthen the governance and risk management practices of large national banks.[3] These heightened expectations reflected the OCC's supervisory experience during the financial crisis and addressed weaknesses the OCC observed in large institutions' governance and risk management practices during this time. Through its work with the Financial Stability Board and Basel Committee on Banking Supervision, the OCC found that many supervisors are establishing, or are considering establishing, similar expectations for the financial institutions they regulate.[4]

In January 2014, the OCC invited public comment on proposed rules and guidelines addressing the following two topics: (i) Guidelines establishing minimum standards for the design and implementation of a Framework for large insured national banks, insured Federal savings associations, and insured Federal branches and minimum standards for boards of directors overseeing the Framework of these institutions (proposed Guidelines); and (ii) the integration of 12 CFR parts 30 and 170 (proposed integration rules and integration guidelines).[5]

After carefully considering the comments we received on the proposed Guidelines, the OCC is adopting these final Guidelines as a new Appendix D to part 30 of our regulations. As described more fully below, the final Guidelines supersede the OCC's previous heightened expectations program with respect to covered banks.[6] The OCC, as the primary financial regulatory agency for national banks and Federal savings associations, believes that the final Guidelines further the goal of the Dodd-Frank Act to strengthen the financial system by focusing management and boards of directors on strengthening risk management practices and governance, thereby minimizing the probability and impact of future crises. In addition, the final Guidelines will provide greater certainty to covered banks about the OCC's risk management expectations and improve examiners' ability to assess compliance with the standards contained in Appendix D. The OCC is also adopting the proposed integration rules and integration guidelines substantially as proposed, with minor technical changes.

We have set forth below a summary of the comments we received, and a detailed description of the proposed Guidelines, significant comments, and the standards contained in the final Guidelines.

Notice of Proposed Rulemaking: Summary of General Comments

The OCC received 25 comment letters on the proposed Guidelines from financial institutions and trade associations, among others, and received no comment letters on the proposed integration rules and integration guidelines. The comments addressed all major sections of the proposed Guidelines. To improve understanding of the issues raised by

[1] Public Law 111–203, 124 Stat. 1376 (2010).

[2] *See, e.g.,* 12 U.S.C. 5365 (requiring enhanced prudential standards for certain bank holding companies and nonbank financial companies).

[3] Further background information on the heightened expectations program is included in the notice of proposed rulemaking entitled *OCC Guidelines Establishing Heightened Standards for Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches; Integration of Regulations.* 79 FR 4282, 4283 (Jan. 27, 2014).

[4] *See* Financial Stability Board, *Thematic Review on Risk Governance* Peer Review Report (Feb. 12, 2013); *Principles for An Effective Risk Appetite Framework* (Nov. 18, 2013). *See also* Basel Committee on Banking Supervision, *Principles for effective risk data aggregation and risk reporting* (Jan. 2013).

[5] 79 FR 4282 (Jan. 27, 2014).

[6] The OCC has adopted a definition of the term ''covered bank'' to clarify the scope of the final Guidelines. This definition is discussed in the definitions section of this preamble.

commenters, the OCC met with a number of these commenters to discuss issues relating to the proposed Guidelines, and summaries of these meetings are available on a public Web site.[7]

Many commenters expressed support for the broader goals of the proposed Guidelines. At the same time, other commenters raised concerns with various provisions in the proposed Guidelines. For example, commenters argued that the proposed Guidelines were too prescriptive and requested the OCC to revise the final Guidelines to be more principles-based and to provide additional flexibility in applying the Guidelines to different types of banks.

Some commenters also interpreted the proposed Guidelines as prohibiting banks from utilizing their parent company's risk governance framework and resources. These commenters noted that this could result in conflicting standards, increased risk, and a duplication of systems and resources and urged the OCC to allow the bank to leverage existing holding company risk management processes.

Commenters also generally opposed categorizing certain organizational units as front line units. These commenters noted that organizational units such as legal, human resources, finance, and information technology do not create the types of risk that should be subject to these Guidelines and thus the OCC should not classify them as front line units. Finally, some commenters argued that the proposed Guidelines inappropriately assigned managerial responsibilities to the board of directors that would distract the board from its strategic and oversight role.

As discussed more fully below, the OCC has revised the final Guidelines in response to the issues and information provided by commenters, and has made technical changes to the final rule and guidelines integrating 12 CFR parts 30 and 170. These modifications to the final Guidelines and explanations that address comments are described in the section-by-section description of the final Guidelines.

Enforcement of the Guidelines

The OCC is adopting the final Guidelines pursuant to section 39 of the Federal Deposit Insurance Act (FDIA).[8] Section 39 authorizes the OCC to prescribe safety and soundness standards in the form of a regulation or guidelines. For national banks, these standards currently include three sets of guidelines issued as appendices to part 30 of our regulations. Appendix A contains operational and managerial standards that relate to internal controls, information systems, internal audit systems, loan documentation, credit underwriting, interest rate exposure, asset growth, asset quality, earnings, and compensation, fees and benefits. Appendix B contains standards on information security and Appendix C contains standards that address residential mortgage lending practices. The safety and soundness standards for Federal savings associations are found in Appendices A and B to 12 CFR part 170. Part 30, part 170, and Appendices A and B were issued on an interagency basis and are comparable.[9]

Section 39 prescribes different consequences depending on whether the agency issues regulations or guidelines. Pursuant to section 39, if a national bank or Federal savings association [10] fails to meet a standard prescribed by regulation, the OCC must require it to submit a plan specifying the steps it will take to comply with the standard. If a national bank or Federal savings association fails to meet a standard prescribed by guideline, the OCC has the discretion to require the submission of such a plan.[11] The issuance of these heightened standards as guidelines rather than as a regulation provides the OCC with supervisory flexibility to pursue the course of action that is most appropriate given the specific circumstances of a covered bank's failure to meet one or more standards, and the covered bank's self-corrective and remedial responses.

The OCC has procedural rules contained in part 30 that implement the enforcement remedies prescribed by section 39. Under these provisions, the OCC may initiate the enforcement process when it determines, by examination or otherwise, that a national bank or Federal savings association has failed to meet the standards set forth in the final Guidelines.[12] Upon making that determination, the OCC may request, through letter or Report of Examination, that the national bank or Federal savings association submit a compliance plan to the OCC detailing the steps the institution will take to correct the deficiencies and the time within which it will take those steps. This request is termed a Notice of Deficiency. Upon receiving a Notice of Deficiency from the OCC, the national bank or Federal savings association must submit a compliance plan to the OCC for approval within 30 days.

If a national bank or Federal savings association fails to submit an acceptable compliance plan, or fails materially to comply with a compliance plan approved by the OCC, the OCC may issue a Notice of Intent to Issue an Order pursuant to section 39 (Notice of Intent). The bank or savings association then has 14 days to respond to the Notice of Intent. After considering the bank's or savings association's response, the OCC may issue the order, decide not to issue the order, or seek additional information from the bank or savings association before making a final decision. Alternatively, the OCC may issue an order without providing the bank or savings association with a Notice of Intent. In this case, the bank or savings association may appeal after-the-fact to the OCC, and the OCC has 60 days to consider the appeal and render a final decision. Upon the issuance of an order, a bank or savings association will be deemed to be in noncompliance with part 30. Orders are formal, public documents, and they may be enforced in district court or through the assessment of civil money penalties under 12 U.S.C. 1818.

Description of the OCC's Guidelines Establishing Heightened Standards

The final Guidelines consist of three sections. Section I provides an introduction to the Guidelines, explains the scope of the Guidelines, and defines key terms used throughout the Guidelines. Section II sets forth the minimum standards for the design and implementation of a covered bank's Framework. Section III provides the minimum standards for the board of directors' oversight of the Framework.

[7] *See http://www.regulations.gov/index.jsp#!docketDetail;D=OCC-2014-0001.*

[8] 12 U.S.C. 1831p-1. Section 39 was enacted as part of the Federal Deposit Insurance Corporation Improvement Act of 1991, Public Law 102–242, section 132(a), 105 Stat. 2236, 2267–70 (Dec. 19, 1991).

[9] As discussed further below, the OCC is also adopting final rules and guidelines that make part 30 and its appendices applicable to Federal savings associations, and that remove part 170.

[10] Section 39 of the FDIA applies to ''insured depository institutions,'' which would include insured Federal branches of foreign banks. While we do not specifically refer to these entities in this discussion, it should be read to include them.

[11] *See* 12 U.S.C. 1831p–1(e)(1)(A)(i) and (ii). In either case, however, the statute authorizes the issuance of an order and the subsequent enforcement of that order in court, independent of any other enforcement action that may be available in a particular case.

[12] For national banks and Federal savings associations, the procedures governing the determination and notification of failure to satisfy a standard prescribed pursuant to section 39, the filing and review of compliance plans, and the issuance, if necessary, of orders are set forth in our regulations at 12 CFR 30.3, 30.4, and 30.5.

Section I: Introduction

Under the proposed Guidelines, the OCC would expect a bank to establish and implement a Framework for managing and controlling the bank's risk taking. The proposed Guidelines established the minimum standards for the design and implementation of the Framework and the minimum standards for the board of directors in overseeing the Framework's design and implementation.

The proposed Guidelines permitted a bank to use its parent company's risk governance framework if the bank has a risk profile that is substantially the same as its parent company's risk profile, the parent company's risk governance framework complies with the proposed Guidelines, and the bank demonstrates through a documented assessment that its risk profile and its parent company's risk profile are substantially the same. The proposed Guidelines provided that the bank should conduct this assessment at least annually or more often in conjunction with the review and update of the Framework performed by independent risk management as set forth in paragraph II.A. of the proposed Guidelines.

Under the proposed Guidelines, a parent company's and bank's risk profiles would be considered substantially the same if, as of the most recent quarter-end Federal Financial Institutions Examination Council Consolidated Reports of Condition and Income (Call Report), the following conditions are met: (i) The bank's average total consolidated assets represent 95 percent or more of the parent company's average total consolidated assets; (ii) the bank's total assets under management represent 95 percent or more of the parent company's total assets under management; and (iii) the bank's total off-balance sheet exposures represent 95 percent or more of the parent company's total off-balance sheet exposures. As provided in the proposed Guidelines, a bank that did not satisfy this test could submit to the OCC for consideration an analysis that demonstrates that the risk profile of the parent company and the bank are substantially the same based on other factors.

The proposed Guidelines provided that the bank would need to develop its own Framework if the parent company's and bank's risk profiles are not substantially the same. The bank's Framework should ensure that the bank's risk profile is easily distinguished and separate from its parent company's for risk management and supervisory reporting purposes and that the safety and soundness of the bank is not jeopardized by decisions made by the parent company's board of directors or management.

Several commenters argued that it was inefficient and counterproductive to require a bank to create a second risk framework in addition to the parent company's framework. According to the commenters, a separate bank-specific risk framework would be isolated from the overall enterprise risk framework and undermine the goals of sound risk management. Other commenters indicated that banks should be allowed to use their parent company's risk governance framework because the Dodd-Frank Act requires bank holding companies to serve as a source of strength for their insured depository institution subsidiaries.

Some commenters also interpreted the proposed Guidelines to prohibit the bank from using any components of the parent company's risk governance framework unless the risk profiles of the bank and its parent holding company are substantially the same. Commenters argued that the OCC should change the threshold for the substantially the same determination from 95 percent to 85 percent. They noted that in certain other regulatory contexts special treatment is granted when the total assets of an insured depository institution comprise 85 percent or more of the assets of its parent company.[13] One commenter argued that the current Call Report and holding company reporting forms do not contain parallel line items for assets under management and off-balance sheet exposures, making it problematic to establish that a bank is above the 95 percent threshold under those measures. Several commenters also suggested that the OCC should allow multiple subsidiary banks of a parent company to aggregate their asset sizes in order to meet the 95 percent threshold. The commenters noted that some banking organizations conduct banking activities through multiple charters and that a prohibition on aggregation would result in unnecessary and duplicative risk management programs.

The OCC is making a few modifications to the introductory section. The final Guidelines continue to establish minimum standards for the design and implementation of a covered bank's Framework and minimum standards for the covered bank's board of directors in providing oversight of the Framework's design and implementation. The OCC notes that these standards are not intended to be exclusive, and that they are in addition to any other applicable requirements in law or regulation. For example, the OCC expects covered banks to continue to comply with the operational and management standards articulated in Appendix A to part 30, including those related to internal controls, internal audit systems, risk management, and management information systems.

Paragraph 3. of the final Guidelines clarifies that a covered bank may use its parent company's risk governance framework in its entirety, without modification, if the framework meets these minimum standards and the risk profiles of the parent company and the covered bank are substantially the same as demonstrated through a documented assessment. The covered bank should conduct this assessment at least annually in conjunction with the review and update of the Framework performed by independent risk management pursuant to paragraph II.A.

Paragraph 4. of the final Guidelines continues to set forth the substantially the same test, but simplifies the test by removing the provisions relating to assets under management and off-balance sheet exposures. Under the final Guidelines, a parent company's and covered bank's risk profiles are substantially the same if, as reported on the covered bank's Call Report for the four most recent consecutive quarters, the covered bank's average total consolidated assets represent 95 percent or more of the parent company's average total consolidated assets.[14] The final Guidelines also provide that a covered bank that does not satisfy this test may submit a written analysis to the OCC for consideration and approval that demonstrates that the risk profile of the parent company and the covered bank are substantially the same based upon other factors.

The OCC has determined not to lower the 95 percent threshold, as suggested by some commenters. The 95 percent threshold in the final Guidelines functions as a safe harbor, above which a covered bank will not need to create its own Framework. If a covered bank and its parent company have substantially the same risk profile, the covered bank can use any and all components of the parent company's risk governance framework as its own, provided the parent company's framework complies with the final

[13] *See, e.g.,* 12 CFR 243.4(a)(3)(i)(B).

[14] The final Guidelines clarify that average total consolidated assets for a parent company means the average of the parent company's total consolidated assets, as reported on the parent company's Form FR Y–9C to the Board of Governors of the Federal Reserve System (Board), or equivalent regulatory report, for the four most recent consecutive quarters.

Guidelines. A covered bank that does not meet the 95 percent threshold can use components of its parent company's framework, provided those components meet the criteria outlined in the Guidelines.

The OCC believes a high threshold is necessary to ensure that a covered bank's Framework appropriately considers the sanctity of each national bank or Federal savings association charter within a parent company's legal entity structure. During the financial crisis, the OCC and some boards of directors were unable to accurately assess certain national banks' risk profiles because their respective parent company's risk management practices were assessing, managing, and reporting risks by line of business, rather than legal entity. In addition, decisions by some parent companies' boards of directors and management teams leading up to the crisis created unacceptable risk levels in their national bank subsidiaries. As a result, these parent companies were unable to provide financial or other support to their bank subsidiaries despite the fact that a parent company is expected to serve as a source of strength for its bank subsidiaries.

The covered bank's Framework should ensure that the covered bank's risk profile is easily distinguished and separate from its parent company for risk management and supervisory reporting purposes and that the safety and soundness of the covered bank is not jeopardized by decisions made by the parent company's board of directors and management. This includes ensuring that assets and businesses are not transferred into the covered bank from nonbank entities without proper due diligence and ensuring that complex booking structures established by the parent company protect the safety and soundness of the covered bank.

Although the final Guidelines continue to provide that a covered bank should establish its own Framework when the parent company's and covered bank's risk profiles are not substantially the same, the Guidelines also clarify that even in these cases a covered bank may, in consultation with the OCC, incorporate or rely on components of its parent company's risk governance framework when developing its own Framework to the extent those components are consistent with the objectives of these Guidelines. It is important to note that neither the proposed Guidelines nor the final Guidelines prohibit a covered bank from using those components of its parent company's risk governance framework that are appropriate for the covered bank. Indeed, the OCC encourages covered banks to leverage their parent company's risk governance framework to the extent appropriate, including using employees of the parent company. For example, it may be appropriate for the same individual to serve as Chief Risk Executive or Chief Audit Executive of a covered bank and its parent company.

We note that the extent to which a covered bank may use its parent company's framework will vary depending on the circumstances. For example, it may be appropriate for a covered bank to use the parent company's framework without modification where there is significant similarity between the covered bank's and parent company's risk profiles, or where the parent company's framework provides for focused governance and risk management of the covered bank. Conversely, a covered bank may incorporate fewer components of the parent company's framework where the risk profiles of the covered bank and parent are less similar, or the parent company's risk governance framework is less focused on the covered bank. In these situations, it may be necessary to modify components of the parent company's risk governance framework that the covered bank incorporates or relies on to ensure the bank's risk profile is easily distinguished from that of its parent and that decisions made by the parent do not jeopardize the safety and soundness of the covered bank. It is expected that the covered bank will consult with OCC examiners to determine which components of a parent company's risk governance framework may be used to ensure that the covered bank's Framework complies with the Guidelines.

The OCC recognizes that covered banks operate within their overall parent company's risk governance framework, and that covered banks may realize efficiencies when their parent company's risk governance framework is consistent with these Guidelines. However, modifications may be necessary when the parent company's risk management objectives are different than the covered bank's risk management objectives. For example, a parent company's board of directors and management will need to understand and manage aggregate risks that cross legal entities, while a covered bank's board and management will need to understand and manage only the covered bank's individual risk profile. The OCC believes these distinct goals and processes are complementary. The covered bank should work closely with its parent company to promote efficiencies and synergies between the two risk governance frameworks.

Scope and Compliance Date

The proposed Guidelines applied to a bank with average total consolidated assets equal to or greater than $50 billion as of the effective date of the Guidelines (calculated by averaging the bank's total consolidated assets, as reported on the bank's Call Reports, for the four most recent consecutive quarters). For those banks with average total consolidated assets less than $50 billion as of the effective date of the Guidelines, but that subsequently have average total consolidated assets of $50 billion or greater, the proposed Guidelines applied to such banks on the as-of date of the most recent Call Report used in the calculation of the average.

Several commenters objected to the $50 billion threshold. Some commenters suggested that the OCC increase the threshold to one more consistent with the complexity of the bank and the heightened risk the bank posed. One commenter suggested using the $250 billion threshold in the Basel III advanced approaches.[15] Another commenter favored eliminating the $50 billion threshold and instead adopting a principles-based approach that applies the Guidelines to banks whose operations are highly complex or present a heightened risk.

Some commenters requested that the OCC provide banks not previously subject to the OCC's heightened expectations program with a year or longer to comply with the final Guidelines. Other commenters argued that the OCC should permit an institution that becomes newly subject to the Guidelines a minimum of two years to achieve full compliance. Several commenters argued that the OCC should allow banks previously subject to the OCC's heightened expectations program a minimum of one year from the date of the final Guidelines because of the new and more detailed requirements contained in the Guidelines.

The OCC believes that the final Guidelines should apply to any bank with average total consolidated assets equal to or greater than $50 billion,[16]

[15] *See* 12 CFR 3.100(b)(1)(i).

[16] The approach for calculating average total consolidated assets under the final Guidelines is the same as that in the proposed Guidelines. Specifically, the final Guidelines provide that average total consolidated assets for a covered bank means the average of the covered bank's total consolidated assets, as reported on the covered bank's Call Reports for the four most recent consecutive quarters.

but recognizes that covered banks with assets equal to or greater than $50 billion may differ in the degree of risk they present and, therefore, as described below, we are making several changes to this section to address the compliance date for covered banks based on size and experience with the heightened expectations program. In addition, we note that the $50 billion asset criteria is a well understood threshold that the OCC and other Federal banking regulatory agencies have used to demarcate larger, more complex banking organizations from smaller, less complex banking organizations.[17] Accordingly, the final Guidelines retain the $50 billion threshold.

The OCC is also clarifying that the final Guidelines will apply to any bank with average total consolidated assets less than $50 billion in the limited circumstances where that institution's parent company controls at least one covered bank.[18] This would include both sister banks of the covered bank as well as covered bank subsidiaries and sister bank subsidiaries that are banks (*e.g.,* insured credit card banks or insured trust banks). The meaning of the terms ''bank,'' ''covered bank,'' and ''control'' is discussed in the Definitions section below.

As noted above, the final Guidelines contain a schedule that phases-in the date for a covered bank to comply with the final Guidelines. A covered bank with average total consolidated assets equal to or greater than $750 billion should comply with the final Guidelines by the effective date, *i.e.,* 60 days after these Guidelines are published in the **Federal Register**. A covered bank with average total consolidated assets equal to or greater than $100 billion but less than $750 billion as of the effective date should comply with the final Guidelines within six months from the effective date.

A covered bank with average total consolidated assets equal to or greater than $50 billion but less than $100 billion as of the effective date should comply with these Guidelines within 18 months from the effective date. A covered bank with average total consolidated assets less than $50 billion that is a covered bank because that bank's parent company controls at least one other covered bank as of the effective date should comply with these Guidelines on the same date that such other covered bank should comply. Finally, a covered bank with less than $50 billion in average total consolidated assets on the effective date of the final Guidelines that subsequently becomes subject to the Guidelines because its average total consolidated assets are equal to or greater than $50 billion should comply with the Guidelines within 18 months from the as-of date of the most recent Call Report used in the calculation of the average.[19] The OCC notes that larger institutions have been subject to the OCC's heightened expectations program since 2010 and should need less time to comply with the final Guidelines. Other covered banks have been subject to certain aspects of the heightened expectations program and therefore may require additional time to comply with all aspects of the final Guidelines.

Reservation of Authority

In order to maintain supervisory flexibility, the proposed Guidelines reserved the OCC's 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 proposed Guidelines provided that the OCC would consider the complexity of products and services, risk profile, and scope of operations to determine whether a bank's operations are highly complex or present a heightened risk.

Conversely, the proposed Guidelines also reserved the OCC's authority to delay the application of the Guidelines to any bank, or modify the Guidelines as applicable to certain banks. Additionally, the proposed Guidelines provided that the OCC may determine that a bank is no longer required to comply with the Guidelines. The OCC would generally make this determination if a bank's operations are no longer highly complex or no longer present a heightened risk that would require continued compliance with the Guidelines. Finally, the proposal provided that the OCC would apply notice and response procedures, when appropriate, consistent with those set out in 12 CFR 3.404 when exercising any of these reservations of authority.

Some commenters expressed concern about the OCC's use of reservation of authority to apply the Guidelines to banks below the $50 billion threshold, particularly community banks. Other commenters asserted that the proposed Guidelines should apply to a bank below the $50 billion threshold only when the bank's risk profile is elevated and the bank has met a list of objective factors.

After reviewing the comments, the OCC is finalizing the reservation of authority paragraph substantially as proposed with minor technical changes. The final Guidelines provide that the OCC reserves the authority to apply the Guidelines, in whole or in part, to a bank below the $50 billion threshold if the OCC determines that the bank's operations are highly complex or otherwise present a heightened risk. The OCC expects to utilize this authority only if a bank's operations are highly complex relative to its risk-management capabilities, and notes that ''[t]his is a high threshold that only will be crossed in extraordinary circumstances.''[20] The OCC does not intend to exercise this reservation of authority to apply the final Guidelines to community banks.[21]

Consistent with the proposal, the final Guidelines reserve the OCC's authority to extend the time for compliance with the Guidelines, modify the Guidelines, or to determine that compliance with the Guidelines is no longer appropriate for a particular covered bank. The OCC would generally make this determination if a covered bank's operations are no longer highly complex or no longer present a heightened risk based on consideration of the factors articulated in the Guidelines. The final Guidelines continue to provide that the OCC will apply notice and response procedures, when appropriate, consistent with those set out in 12 CFR

[17] *See* 12 CFR 46.1 (stress testing); 12 CFR 252.30 (enhanced prudential standards for bank holding companies with total consolidated assets of $50 billion or more).

[18] The OCC notes that many of the covered banks it regulates are part of a larger holding company structure that includes smaller OCC-supervised insured depository institutions. In some instances, the OCC has observed that a covered bank's parent company does not pay sufficient attention to the operations of these smaller entities. The OCC is expressly including these smaller entities in the definition of ''covered bank'' because the OCC believes that a covered bank's parent company should devote adequate attention to assessing and managing the risk associated with these entities' activities. The OCC notes that, as with covered banks with average total consolidated assets of $50 billion or more, these smaller banks may incorporate or rely on appropriate components of their parent company's risk governance framework.

[19] Once a covered bank becomes subject to the final Guidelines because its average total consolidated assets have reached or exceeded the $50 billion threshold, it is required to continue to comply with the Guidelines even if its average total consolidated assets subsequently drop below $50 billion, unless the OCC determines otherwise and exercises its reservation of authority as discussed below.

[20] The Honorable Thomas J. Curry, Comptroller of the Currency, Address at the American Bankers Association Risk Management Forum (Apr. 10, 2014).

[21] *See id.* (''Some community bankers may be reading that language as a loophole that we will use to impose onerous new requirements on community banks. I want to assure you that this is not the case and not our intent.'').

3.404 when exercising any of these reservations of authority.

Insured Federal Branches

As discussed above, the proposed Guidelines applied to an insured Federal branch of a foreign bank with average total consolidated assets of $50 billion or more. We noted in the preamble to the proposed Guidelines that, pursuant to the reservation of authority, the OCC may modify the Guidelines to tailor them for insured Federal branches due to their unique nature.

Some commenters requested that the OCC delay any decision regarding application of the Guidelines to an insured Federal branch pending a more definite determination of what such tailoring contemplates. In particular, these commenters requested that the OCC clarify the treatment of independent risk management and internal audit, and the role for the foreign bank's governing body under the Guidelines. Some commenters also asserted that the proposed Guidelines did not adequately address that an insured Federal branch does not have a board of directors. Some commenters also argued that the final Guidelines should provide each insured Federal branch considerable flexibility to apply them in a manner best suited to its circumstances.

After reviewing the comments, the OCC has determined that the final Guidelines will apply to insured Federal branches with $50 billion or more in average total consolidated assets. However, the OCC recognizes that insured Federal branches do not have a U.S. board of directors and that their risk governance frameworks will vary due to the variety of activities performed in the branch. As a result, the OCC intends to apply the final Guidelines in a flexible manner to insured Federal branches. For example, if an insured Federal branch were to become subject to these final Guidelines, the OCC would apply the Guidelines in a manner that takes into account the nature, scope, and risk of the branch's activities. This means that the OCC will consult with the insured Federal branch to adapt the final Guidelines in an appropriate manner to the branch's operations.

In addition, the final Guidelines omit footnote one from the proposal which provided that, in the case of an insured Federal branch, the board of directors means the managing official in charge of the branch. In the event an insured Federal branch becomes subject to the final Guidelines, OCC examiners will consult with the branch to determine the appropriate person or committee to undertake the responsibilities assigned to the board of directors under the final Guidelines. The OCC continues to expect that all Federal branches have risk governance frameworks in place that are commensurate with the level of risk taken in or outside the U.S. impacting U.S. operations.

Preservation of Existing Authority

As discussed above, the final Guidelines are enforceable pursuant to section 39 of the FDIA and part 30 of our rules. Section I of the Guidelines also provides that nothing in section 39 or the Guidelines in any way limits the authority of the OCC to address unsafe or unsound practices or conditions or other violations of law.

Definitions

The proposed Guidelines defined several terms, including Chief Audit Executive, Chief Risk Executive, front line unit, independent risk management, internal audit, risk appetite, and risk profile. With the exception of the front line unit definition, the OCC is adopting these definitions substantially as proposed, with certain clarifying and technical changes. The final Guidelines also include definitions for the terms bank, control, and covered bank.

Bank. The proposed Guidelines defined the term ''bank'' in the scope section of the proposed Guidelines [22] to mean any insured national bank, insured Federal savings association, or insured Federal branch of a foreign bank with average total consolidated assets equal to or greater than $50 billion as of the effective date of the Guidelines. The OCC is moving this definition to paragraph I.E. Definitions to consolidate all of the definitions in one location. Under the final Guidelines, the term ''bank'' means any insured national bank, insured Federal savings association, or insured Federal branch of a foreign bank. As discussed below, the OCC is also introducing the term ''covered bank'' to more clearly indicate the types of institutions covered by these Guidelines.

Chief Audit Executive. The proposed Guidelines defined the term ''Chief Audit Executive'' (CAE) as an individual who leads internal audit and is one level below the Chief Executive Officer (CEO) in the bank's organizational structure. The OCC received no comments and is adopting this definition as proposed with one technical change.

Chief Risk Executive. The proposed Guidelines defined the term ''Chief Risk Executive'' (CRE) as an individual who leads an independent risk management unit and is one level below the CEO in the bank's organizational structure. The proposal noted that some banks designate one CRE, while others designate risk-specific CREs.[23] In the latter situation, the proposal provided that the bank should have a process for coordinating the activities of all independent risk management units so they can provide an aggregated view of risks to the CEO and the board of directors or the board's risk committee. The proposal solicited comment on the advantages and disadvantages of having a single CRE versus having multiple, risk-specific CREs.

Commenters disagreed on this issue. Some commenters noted that it is advantageous for a single CRE to provide oversight to all independent risk management units, and argued that a single CRE is necessary to ensure a cohesive and coordinated approach to risk management. Other commenters asserted that requiring a single CRE would be too prescriptive for the varied risk profiles and organizational designs among banks, and noted that such a requirement may not be appropriate to the size, scale, and complexity of each institution. In addition, these commenters noted that having two or three executives performing CRE functions and having access to the board of directors can provide additional perspective to the board.

After reviewing the comments received, the OCC is adopting the definition substantially as proposed with one clarifying change. The final Guidelines provide that Chief Risk Executive means an individual who leads an independent risk management unit and is one level below the CEO in a covered bank's organizational structure.[24] The final definition expressly states that a covered bank may have more than one CRE. Because the OCC did not receive compelling information regarding the appointment of a single CRE, we are providing covered banks flexibility in determining the appropriate number of CREs. The OCC continues to believe, however, that a covered bank with multiple, risk-specific CREs should have effective processes for coordinating the activities of all independent risk management units so that they can provide an aggregated view of all risks to the CEO

[22] *See* proposed Guidelines I.A.

[23] *See* 79 FR 4282, 4285 n.15 (Jan. 27, 2014).

[24] *See* final Guidelines paragraph I.E.3.

and the board of directors or the board's risk committee.

Control. As discussed below, the OCC is adopting a definition of the term ''covered bank'' to clarify the scope of the final Guidelines. The definition of the term ''covered bank'' turns, in part, on the definition of ''control.'' While the concept of control was discussed in the proposed Guidelines,[25] the proposal did not include a definition of this term.

The OCC is adopting a definition of the term ''control'' that is based on the definition provided in 12 CFR 3.2. Under the final Guidelines, a parent company controls a covered bank if it: (i) Owns, controls, or holds with power to vote 25 percent or more of a class of voting securities of the covered bank; or (ii) consolidates the covered bank for financial reporting purposes. The OCC believes that this definition will assist institutions in determining whether they are a ''covered bank,'' and therefore subject to the final Guidelines.

Covered Bank. In order to clarify the scope of the final Guidelines, the OCC is adopting a definition of the term covered bank. Under the final Guidelines, the term covered bank means any bank: (i) With average total consolidated assets equal to or greater than $50 billion; (ii) with average total consolidated assets less than $50 billion if that bank's parent company controls at least one covered bank; or (iii) with average total consolidated assets less than $50 billion, if the OCC determines that the bank's operations are highly complex or otherwise present a heightened risk as to warrant the application of the final Guidelines. The OCC believes that this definition accurately reflects the scope of the proposed Guidelines, and has made changes throughout the text of the Guidelines to incorporate this term.

Front line unit. The proposed Guidelines defined the term ''front line unit'' as any organizational unit within the bank that: (i) Engages in activities designed to generate revenue for the parent company or bank; (ii) provides services, such as administration, finance, treasury, legal, or human resources to the bank; or (iii) provides information technology, operations, servicing, processing, or other support to any organizational unit covered by the proposed Guidelines.[26]

Several commenters strongly opposed this definition claiming that it inappropriately includes organizational units that do not ''own'' or create risk, such as legal, compliance, finance, human resources, and information technology. These commenters suggested that these types of organizational units mainly perform risk mitigation or support functions and therefore should not be subject to the standards in the Guidelines. Other commenters expressed concern that the proposed definition would subordinate the views of these types of organizational units to independent risk management thus, for example, potentially subjecting legal decisions and advice to review by independent risk management and internal audit.

Some commenters also noted that organizational units may have many different functions, only some of which involve accountability for risk that warrants treatment under these Guidelines. One commenter suggested that, in such cases, the OCC classify part of the unit as a front line unit. One commenter suggested that the front line unit definition should include revenue-generating business units and personnel who provide functional support to these units, such as legal advisory services or technology development, when those personnel are compensated by and report into the business unit. Finally, several commenters urged the OCC to provide flexibility to determine how service and support functions should fit into the bank's risk governance framework.

After carefully considering the comments, the OCC is making several changes to this definition. Under the final Guidelines, a front line unit means, except as otherwise provided, any organizational unit or function thereof in a covered bank that is accountable for one of several enumerated risks[27] and that either: (i) Engages in activities designed to generate revenue or reduce expenses for the parent company or covered bank; (ii) provides operational support or servicing to any organizational unit or function within the covered bank in the delivery of products or services to customers; or (iii) provides technology services to any organizational unit or function covered by these Guidelines. Thus, to meet the definition of a front line unit, an organizational unit or function would need to be accountable for a risk and also meet one of three additional criteria that capture the types of risk-taking activities these Guidelines are intended to address. The final Guidelines also provide that a front line unit does not ordinarily include an organizational unit or function thereof within a covered bank that provides legal services to the covered bank.

The OCC believes that this revised definition provides greater flexibility to identify and classify organizational units or functions thereof that are responsible for risks covered by these Guidelines as front line units. Specifically, this definition makes it possible for part of an organizational unit to qualify as a front line unit without implicating the entire organizational unit. For example, in some institutions, the Chief Financial Officer's organizational unit may be responsible for setting goals and providing oversight to enterprise-wide expense reduction initiatives. These initiatives have the potential to create one or more risks, if actions taken to achieve cost saving goals inappropriately weaken risk management practices or internal controls. With regard to this responsibility, the finance organizational unit would be a front line unit, subject to the oversight and challenge of independent risk management. However, the finance organizational unit would not be a front line unit with regard to its responsibility to establish, assess, or report on line of business compliance with other enterprise-wide policies and procedures, such as those associated with preparing the covered bank's financial statements.

The final definition also clarifies that, if an organizational unit or function is accountable for a risk within a covered bank, it is considered a front line unit whether or not it created the risk. The purpose of this change is to make clear that a front line unit's responsibility for, or ownership of, a risk may arise by engaging in the activity that originally created the risk within the covered bank, or when the organizational unit is assigned accountability for a risk that was created by another organizational unit. For example, accountability for an individual loan or a portfolio of loans and its associated risks may transfer from one organizational unit or function to another within a covered bank. The organizational unit or function that assumes responsibility for the loan or loan portfolio becomes a front line unit

[25] *See* 79 FR 4285.

[26] *See* proposed Guidelines I.C.3. The proposal clarified that servicing includes activities done in support of front line lending units, such as collecting monthly payments, forwarding principal and interest payments to the current lender in the event a loan has been sold, maintaining escrow accounts, paying taxes and insurance premiums, and taking steps to collect overdue payments. The proposal also provided that processing refers to activities such as item processing (*e.g.,* sorting of checks), inputting loan, deposit, and other contractual information into information systems, and administering collateral tracking systems. *See* 79 FR 4286 n.17–18.

[27] These risks are credit risk, interest rate risk, liquidity risk, price risk, operational risk, compliance risk, strategic risk, or reputation risk, as described in the ''Large Bank Supervision'' booklet of the *Comptroller's Handbook* (Jan. 2010).

at the time accountability for the risk is transferred.

Conversely, there may be circumstances where an organizational unit may have some accountability for one or more risks, but may not meet other provisions of the definition and thus would not be a front line unit for purposes of these Guidelines. For example, one of the primary responsibilities of human resources is to design and implement compensation programs, which, if not designed and implemented properly, could motivate inappropriate risk-taking behavior. However, human resources does not meet any of the three additional criteria, and therefore, is not a front line unit for purposes of these Guidelines. The OCC believes excluding human resources from the definition of front line unit is appropriate, given that the compensation programs it designs and implements are designed with input from other organizational units and subject to the review and approval of the board of directors, or a committee thereof. The board of directors may, at its discretion, request input from independent risk management on the design and implementation of the compensation program or individual compensation plans, regardless of whether human resources is a front line unit. Furthermore, the other activities in which human resources engages are not directly related to the types of risks covered by these Guidelines.

The proposed Guidelines provided that an organizational unit that engages in activities designed to generate revenue for the parent company or the bank would be a front line unit. The final Guidelines modify this provision to provide that a front line unit could include an organizational unit or function that engages in activities designed to generate revenue or ''reduce expenses.'' The purpose of this change is to more effectively include within the front line unit definition certain functions within an organizational unit without including the entire unit.

Under the proposal, a front line unit included an organizational unit that ''provides information technology, operations, servicing, processing, or other support to any organizational unit covered by these Guidelines.'' The OCC notes that, in the revised definition, an organizational unit or function accountable for risk may be a front line unit if it ''provides operational or servicing support to any organizational unit or function within the covered bank in the delivery of products or services to customers.'' The OCC revised this definition because the proposed definition was too broad and could create issues similar to those raised by commenters with regard to including all aspects of organizational units such a finance, human resources, etc., in the front line unit definition. The revised definition is more focused on the organizational units and functions that the OCC intended to include in the definition of front line unit.

Finally, the OCC agreed with commenters that the definition of a front line unit should not ordinarily include an organizational unit or function thereof that provides legal services to the covered bank. The OCC notes, however, that there may be instances where the General Counsel is responsible for functions that extend beyond legal services. The OCC expects that examiners will determine whether these functions meet the definition of a front line unit, independent risk management, or internal audit and will discuss with covered banks whether any determinations made by the covered bank conflict with the final Guidelines.

Independent risk management. The proposed Guidelines defined the term independent risk management as any organizational unit within the bank that has responsibility for identifying, measuring, monitoring, or controlling aggregate risks. The proposal noted that these units maintain independence from front line units by following the reporting structure specified in the proposed Guidelines. Under the proposal's reporting structure, the board of directors or the board's risk committee reviews and approves the Framework and any material policies established under the Framework. In addition, the board of directors or the board's risk committee approves all decisions regarding the appointment or removal of the CRE and approves the annual compensation and salary adjustment of the CRE. The proposal clarified that the board of directors or the board's risk committee should receive communications from the CRE on the results of independent risk management's risk assessments and activities, and other matters that the CRE determines are necessary.[28] The proposal also provided that the board of directors or its risk committee should make appropriate inquiries of management or the CRE to determine whether there are scope or resource limitations that impede the ability of independent risk management to execute its responsibilities.[29]

The proposed definition specified that the CEO oversees the CRE's day-to-day activities. The proposal clarified that this includes resolving disagreements between front line units and independent risk management that cannot be resolved by the CRE and front line unit(s) executive(s), and overseeing budgeting and management accounting, human resources administration, internal communications and information flows, and the administration of independent risk management's internal policies and procedures.[30] Finally, the proposed definition provided that no front line unit executive oversees any independent risk management unit.

Some commenters noted that the proposed Guidelines suggest that cooperative or integrated relationships between independent risk management and front line units could undermine the independence of independent risk management. These commenters argued that independent risk management's effectiveness can be enhanced through active involvement with business units, and that the final Guidelines should recognize the benefits of, and not create impediments to, this engagement.

Commenters also addressed the relationship between a parent company's and bank's independent risk management functions. Some commenters noted that the proposal conflicts with other regulatory authorities insofar as those authorities expect risk officers at the bank to report into the parent company's risk management function, whereas the proposal provided that the CRE of the bank should report to a bank's CEO. Other commenters expressed the view that the proposed Guidelines appear to require a bank to have a separate chief risk officer and separate risk management organization from its parent company. These commenters argued that requiring risk management activities at the bank separately from the same activities at the parent company would be duplicative and increase compliance costs.

One commenter noted that the provision regarding the CEO's oversight of the CRE's day-to-day activities suggested too prescriptive a level of involvement. This commenter noted that while the CEO should be accountable for these activities, he or she should not be required to be personally involved in the day-to-day activities of other executives. This commenter requested the OCC to clarify that the CEO should not be expected to become significantly involved in the details of independent risk management.

[28] 79 FR 4287.

[29] *Id.*

[30] *Id.*

The OCC is adopting the definition substantially as proposed with certain modifications to address commenters' concerns. The final Guidelines provide that independent risk management means any organizational unit within a covered bank that that has responsibility for identifying, measuring, monitoring, or controlling aggregate risks.[31]

Consistent with the proposal, the final Guidelines articulate a reporting structure that enables independent risk management to maintain its independence from front line units.[32] Under this reporting structure, the board of directors or the board's risk committee reviews and approves the Framework. In addition, the final Guidelines clarify that a CRE should have unrestricted access to the board of directors and its committees with regard to risks and issues identified through independent risk management's activities. The board of directors or its risk committee approves all decisions regarding the appointment or removal of the CREs and approves the annual compensation and salary adjustment of the CREs. The final definition removes the provision for the CEO to oversee the CRE's (or CREs') day-to-day activities. The term day-to-day activities was intended to convey that the CEO would oversee the CRE's (or CREs') activities in a manner similar to the oversight the CEO provides to other direct reports. Given the potential for misinterpretation of the term day-to-day, and the fact that this expectation is implied in the CRE's (or CREs') reporting structure defined in the Guidelines, the OCC determined that this additional requirement is not necessary. The final Guidelines continue to provide that no front line unit executive oversees any independent risk management unit. Conversely, the CRE should not oversee any front line unit.

The OCC has also removed from the final definition the provision that the board of directors or the board's risk committee review and approve any material policies established under the Framework. As discussed below, the OCC did not intend to assign managerial responsibilities to the board of directors or its risk committee. The OCC believes that board or risk committee approval of material policies under the Framework would be burdensome, and that these policies should be approved by management instead. Nevertheless, the OCC continues to believe that the board of directors or the board's risk committee should receive communications from the CRE on the results of independent risk management's risk assessments and activities, and other matters that the CRE determines are necessary. In addition, the board of directors or its risk committee should make appropriate inquiries of management or the CRE to determine whether there are scope or resource limitations that impede the ability of independent risk management to execute its responsibilities.

The OCC did not intend the proposed Guidelines to limit interaction between independent risk management and front line units, nor did the OCC intend to imply that the relationship between front line units and independent risk management should be uncooperative or adversarial. Instead, the OCC expects independent risk management to coordinate and to actively engage with front line units. However, the OCC expects that independent risk management will apply its own judgment when assessing risks and the effectiveness of risk management practices within a front line unit. In addition, there may be situations where independent risk management and front line units disagree. As provided in the proposal, the OCC continues to believe that these disagreements should be resolved by the CEO when the CRE and front line unit(s) executive(s) are unable to resolve these issues.

The Guidelines, as proposed and finalized, do not limit or prevent an employee of a covered bank, such as a CRE, from also serving as an officer with the covered bank's parent company and satisfying reporting requirements applicable to the covered bank's parent company. Accordingly, if a CRE is also an employee of a covered bank's parent company, the final Guidelines do not prohibit the CRE from reporting to an executive within the parent company provided that the executive does not impede the CRE's independence within the covered bank's Framework. Similarly, as discussed above, the OCC notes that the final Guidelines clarify that a covered bank may use elements of a parent company's risk governance framework, but only to the extent that this is appropriate for the covered bank.

Internal audit. The proposed Guidelines defined the term internal audit as the organizational unit within the bank that is designated to fulfill the role and responsibilities outlined in 12 CFR part 30, Appendix A, II.B. Similar to the proposed definition of independent risk management, the proposal noted that internal audit maintains independence from front line units and independent risk management units by implementing the reporting structure specified in the proposed Guidelines. Under the proposal's reporting structure, the board's audit committee reviews and approves internal audit's overall charter, risk assessments, and audit plans. In addition, the proposal provided that the audit committee approves all decisions regarding the appointment or removal and annual compensation and salary adjustment of the CAE. The proposal clarified that the audit committee should receive communications from the CAE on the results of internal audit's activities or other matters that the CAE determines are necessary and make appropriate inquiries of management or the CAE to determine whether there are scope or resource limitations that impede the ability of internal audit to execute its responsibilities.[33]

The proposed definition also provided that the CEO oversees the CAE's day-to-day activities. The proposal clarified that the CEO's oversight responsibilities include, but are not limited to, budgeting and management accounting, human resources administration, internal communications and information flows, and the administration of the unit's internal policies and procedures.[34] The proposed definition also noted that in some banks, the audit committee may assume the CEO's responsibilities to oversee the CAE's day-to-day activities, and that this would be acceptable under the proposed Guidelines.[35] Finally, the proposed definition provided that no front line unit executive oversees internal audit.

Similar to comments on the proposed definition of independent risk management, comments on the proposed definition of internal audit focused on the organizational unit's reporting structure. Some commenters argued that the reporting line for the CAE was too narrow and requested that the final Guidelines provide more flexibility to permit the CAE to report to another senior executive (*e.g.,* general counsel) on day-to-day issues. These commenters noted that permitting more flexibility supports the goals of internal audit independence and unfettered access to the bank's board of directors. Other commenters noted that internal audit and the CAE are most effective and independent when they report functionally to the board of directors or the audit committee and administratively to a suitable executive, such as the CEO.

[31] Final Guidelines paragraph I.E.7.

[32] *Id.*

[33] 79 FR 4287.

[34] 79 FR 4288.

[35] *See* proposed Guidelines I.C.5 n.2.

Some commenters also expressed the view that the proposed Guidelines would require a banking organization to establish duplicative audit departments for its parent company and each of its banks. These commenters noted that a centralized audit function is more effective and efficient, ensures consistent audit coverage, and enables enterprise-wide functional reviews that help to identify systemic issues quickly. The OCC did not intend to suggest that a covered bank is prohibited from using its parent company's risk governance framework when their respective risk profiles are not substantially the same. As described more fully above, 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.

One commenter noted that the provision regarding the audit committee's or CEO's oversight of the CAE's day-to-day activities suggested a level of involvement that was too prescriptive and, in the case of the audit committee, too management-oriented. This commenter requested that the OCC modify this provision to recognize that neither the CEO nor audit committee should be expected to become significantly involved in the details of internal audit. Finally, some commenters argued that the audit committee should only review and approve material risk assessments.

After reviewing the comments received, the OCC is adopting the definition of internal audit substantially as proposed with certain modifications. As provided in the final Guidelines, the term internal audit means the organizational unit within a covered bank that is designated to fulfill the role and responsibilities outlined in 12 CFR part 30, Appendix A, II.B.

Consistent with the proposal, the final Guidelines articulate a reporting structure that enables internal audit to maintain its independence from front line units and independent risk management. Under the reporting structure included in the final Guidelines, the CAE has unrestricted access to the audit committee with regard to risks and issues identified through internal audit's activities. In addition, the audit committee reviews and approves internal audit's overall charter and audit plans. Further, the audit committee approves all decisions regarding the appointment or removal and annual compensation and salary adjustment of the CAE. The final definition clarifies that the audit committee or the CEO oversees the CAE's administrative activities. Finally, the final definition continues to provide that no front line unit executive oversees internal audit.

The OCC agrees with comments that neither the CEO nor the audit committee need to be involved in the details of the CAE's daily activities. The final definition preserves this dual reporting structure, and clarifies that the CEO or the audit committee oversees the CAE's administrative activities, rather than the CAE's day-to-day activities. This reflects the OCC's belief that either the CEO or the audit committee should have primary oversight responsibility over the CAE's administrative activities. These administrative activities include routine personnel matters such as leave and attendance reporting, expense account management, and other departmental matters such as furniture, equipment, and supplies. In addition, revisions made to the definition of front line unit provide internal audit more flexibility to consult with other organizational units, as necessary. For example, the final Guidelines do not prevent internal audit from consulting with a covered bank's legal unit on legal matters because the legal unit is generally not a front line unit.

The OCC recognizes that the proposed definition could have been interpreted to mean that the audit committee should review and approve all internal audit risk assessments, and agrees with commenters that this could impose operational burdens on the audit committee and detract from their oversight role. Therefore, the final definition removes this provision and clarifies that the audit committee reviews and approves the overall charter and audit plan. When presenting the audit plan to the audit committee for approval, internal audit may include the risk assessments that support the audit plan to assist the committee in carrying out its responsibilities. Finally, the OCC continues to expect that the audit committee should receive communications from the CAE on the results of internal audit's activities or other matters that the CAE determines are necessary and make appropriate inquiries of management or the CAE to determine whether there are scope or resource limitations that impede the ability of internal audit to execute its responsibilities.

Parent company. The term ''parent company'' was used throughout the proposed Guidelines. One commenter noted that this term can mean a variety of different entities within a multi-tiered holding company structure.

The OCC is adopting a definition of the term ''parent company'' to clarify the final Guidelines. The term parent company means the top-tier legal entity in a covered bank's ownership structure. Thus, the parent company of a covered bank that is an insured national bank or insured Federal savings association may be a domestic or foreign entity.

Risk appetite. The proposed Guidelines defined the term ''risk appetite'' as the aggregate level and types of risk the board of directors and management are willing to assume to achieve the bank's strategic objectives and business plan, consistent with applicable capital, liquidity, and other regulatory requirements. The OCC received no comments on this definition and is adopting it as proposed with minor technical changes.

Risk profile. The proposed Guidelines defined the term risk profile as a point-in-time assessment of the bank's risks, aggregated within and across each relevant risk category, using methodologies consistent with the risk appetite statement described in II.E. of the proposed Guidelines. The OCC received no comments on this definition and is adopting it as proposed with minor technical changes.

Section II: Standards for Risk Governance Framework

Risk Governance Framework

Section II of the proposed Guidelines set minimum standards for the design and implementation of a bank's Framework. Under paragraphs A. and B., the proposal required a bank to establish and adhere to a formal, written Framework approved by the board of directors or its risk committee that is reviewed and updated at least annually (and as often as needed) by independent risk management to address changes in the bank's risk profile caused by internal or external factors or the evolution of industry risk management practices. We received no comments on this section, however we are making clarifying changes. We have added a provision stating that the Framework should include delegations of authority from the board of directors to management committees and executive officers as well as risk limits established for material activities. The Framework should also include processes for management's reports to the board of directors covering policy, limit compliance, and exceptions. In addition, we have added that the review of the Framework should include changes resulting from emerging risks and the covered bank's strategic plans.

Scope of Risk Governance Framework

Under the proposed Guidelines, the Framework would cover certain specified risk categories that apply to the bank. These categories are credit risk, interest rate risk, liquidity risk, price risk, operational risk, compliance risk, strategic risk, and reputation risk.

One commenter requested clarification regarding the meaning of reputation and strategic risk and argued that the OCC should provide additional clarification or remove these two risk types. The final Guidelines continue to include all eight categories of risk, which are described in existing OCC guidance.[36] The OCC recognizes that industry practices for managing reputation and strategic risks are less developed than those associated with other risk categories. However, it is important for boards of directors and management teams to incorporate these risks into their decision-making processes. Therefore, for purposes of the final Guidelines, the OCC expects front line units, independent risk management, and internal audit to consider these risks when carrying out their responsibilities under the Guidelines.

Roles and Responsibilities

Paragraphs II.C.1. through 3. of the final Guidelines set forth the roles and responsibilities for front line units, independent risk management, and internal audit.[37] These units are fundamental to the design and implementation of the Framework. As we noted in the preamble to the proposed Guidelines, they are often referred to as the ''three lines of defense'' and, together, should establish an appropriate system to control risk taking. These units should keep the board of directors informed of the covered bank's risk profile and risk management practices to allow the board of directors to provide credible challenges to management's recommendations and decisions. In addition, the independent risk management and internal audit units must have unrestricted access to the board, or a committee thereof, with regard to their risk assessments, findings, and recommendations, independent from front line unit management and, when necessary, the CEO. This unrestricted access to the board of directors is critical to the integrity of the Framework.

In carrying out their responsibilities within the Framework, front line units, independent risk management, and internal audit may engage the services of external experts to assist them. This expertise can be useful in supplementing internal expertise and providing perspective on industry practices. However, no organizational unit in the covered bank may delegate its responsibilities under the Framework to an external party.

Many of the commenters expressed support for the lines of defense risk governance structure contained in the proposed Guidelines. Some commenters, however, argued that classifying all of a bank's activities into one of three lines of defense draws artificial bright lines that ignore the mix of functions performed. Other commenters noted that placing all units other than independent risk management and internal audit in the front line could force banks to significantly modify their organizational structures, reporting lines, and risk control practices and that this could impair banks' ability to effectively manage risks. A few commenters asked for additional guidance on the reporting structures for compliance and loan review programs.

As discussed earlier, the OCC has revised the definition of front line unit to provide covered banks more flexibility in identifying front line units. The OCC believes that these revisions respond to commenters' concerns and more closely align the final Guidelines with the traditional ''lines of defense'' approach. Below, we discuss the role and responsibilities of front line units, independent risk management, and internal audit.

Role and Responsibilities of Front Line Units

Front line units are the first of a bank's three lines of defense. The proposed Guidelines provided that front line units should take responsibility and be held accountable by the CEO and the board of directors for appropriately assessing and effectively managing all of the risks associated with their activities. The proposed Guidelines provided that front line units should assess, on an ongoing basis, the material risks associated with their activities. The front line unit should use these risk assessments as the basis for fulfilling the responsibilities that were described in paragraphs (b) and (c) of paragraph II.C.1. of the proposed Guidelines and for determining if they need to take action to strengthen risk management or reduce risk given changes in the unit's risk profile or other conditions.

Paragraph (b) provided that front line units should establish and adhere to a set of written policies that include front line unit risk limits, as discussed in paragraph II.F. of the proposed Guidelines. The proposed Guidelines provided that these policies should ensure that risks associated with the front line units' activities are effectively identified, measured, monitored, and controlled consistent with the bank's risk appetite statement, concentration risk limits, and the bank's policies established within the Framework pursuant to paragraphs II.C.2.(c) and II.G. through K. of the proposed Guidelines.

Paragraph (c) provided that front line units should also establish and adhere to procedures and processes necessary to ensure compliance with the aforementioned written policies. Paragraph (d) provided that front line units should adhere to all applicable policies, procedures, and processes established by independent risk management.

Finally, the proposed Guidelines provided that front line units should develop, attract, and retain talent and maintain appropriate staffing levels, and establish and adhere to talent management processes and compensation and performance management programs that comply with paragraphs II.L. and II.M., respectively, of the proposed Guidelines.

Some commenters expressed concern that the proposed Guidelines prevent front line units from relying on other organizational units to perform their assigned responsibilities. For example, one commenter argued that the proposed Guidelines could be interpreted as suggesting that front line units have exclusive responsibility for establishing risk limits, a responsibility assigned to independent risk management in many banks. This commenter recommended that the final Guidelines clarify that front line units do not have exclusive responsibility for establishing front line unit risk limits, and that the front line unit may perform this responsibility by or in conjunction with independent risk management. Another commenter suggested that the final Guidelines recognize that a front

[36] *See* ''Large Bank Supervision'' booklet of the *Comptroller's Handbook* (Jan. 2010) (describing these risks).

[37] These roles and responsibilities are in addition to any roles and responsibilities set forth in Appendices A, B, and C to Part 30. Many of the risk management practices established and maintained by a covered bank to meet these standards, including loan review and credit underwriting and administration practices, should be components of its Framework, within the construct of the three distinct units identified in the final Guidelines. In addition, existing OCC guidance sets forth standards for establishing risk management programs for certain risks, *e.g.,* compliance risk management. These risk-specific programs should also be considered components of the Framework, within the context of the three units described in paragraph II.C. of the final Guidelines.

line unit may use policies, procedures, and controls established by other organizational units, and that the front line units' responsibility should be contributing their expertise to the development of those policies, procedures and controls. Some commenters also requested the OCC to clarify how the responsibilities assigned to front line units would apply to legal services or other functions that, in some banks, do not report directly to a business leader.

After reviewing the comments, the OCC is adopting the role and responsibilities of front line units with minor clarifying changes. To allow covered banks some flexibility in designing their Framework, the final Guidelines provide that a front line unit may fulfill its responsibilities either alone or in conjunction with another organizational unit whose purpose is to assist a front line unit in fulfilling its responsibilities under the Framework. In such cases, the Framework should establish appropriate authority and accountability for each responsibility in the Framework, and the organizational unit assisting the front line unit cannot be independent risk management. As the OCC observed during the financial crisis, it can be challenging to instill a sense of ''risk ownership'' in a front line unit when multiple organizational units are responsible for the risks associated with the front line unit's activities. Banks whose business leaders viewed themselves as accountable for the risks created through their activities fared better in the crisis than banks where accountability for risks were shared among multiple organizational units. The OCC cautions covered banks that rely on such a structure to be diligent in reinforcing the front line unit's accountability for the risks it creates.

With respect to paragraph (c) of the final Guidelines, a front line unit's processes for establishing its policies should provide for independent risk management's review and approval of these policies to ensure they are consistent with other policies established within the Framework. Within this process, independent risk management would review and approve the front line unit's risk limits. The final Guidelines do not prescribe the process through which independent risk management reviews and approves policies and risk limits. In some covered banks, independent risk management may be involved from the beginning of the process through the final approval and, in other covered banks, the front line unit may develop risk limits internally and submit them to independent risk management for review, challenge, and approval.

The OCC notes that the standards articulated in paragraphs (b) and (c) of the final Guidelines should not be interpreted as an exclusive list of actions front line units should take to manage risk effectively. Front line units should use their ongoing risk assessments to determine if additional actions are necessary to strengthen risk management practices or reduce risk. For example, there may be instances where front line units should take action to manage risk effectively, even if the covered bank has not exceeded its risk limits.

As described above, the OCC has made revisions to the definition of front line unit that the OCC believes address commenters' concerns regarding the application of front line unit responsibilities to legal. Several commenters requested clarification on how compliance fits into the risk governance framework and expressed varying views on whether compliance should be considered a front line unit, independent risk management, internal audit, or a different organizational unit. With regard to compliance, the OCC's guidance is currently outlined in the ''Compliance Management System'' booklet of the *Comptroller's Handbook* and includes responsibilities for all three lines of defense.[38]

Per the *Comptroller's Handbook,* a compliance risk management system ''includes the compliance program and the compliance audit function. . . . The compliance program consists of the policies and procedures which guide employees' adherence to laws and regulations.''[39] Within the Framework, these policies and procedures would generally be the responsibility of the front line unit if they address risks associated with the front line unit's activities or independent risk management if they address bank-wide or aggregate risks. The *Comptroller's Handbook* further states, ''[t]he compliance audit function is independent testing of an institution's transactions to determine its level of compliance with consumer protection laws, as well as the effectiveness of, and adherence with, policies and procedures.''[40] Within the Framework, the independent testing may be performed by independent risk management, internal audit, or both.

As noted previously, a few commenters asked for additional guidance on the reporting structure for the loan review function.[41] Within the Framework, the loan review function may report to either the second or third line of defense. The loan review function should not report to the executive officer who establishes and oversees front line unit credit policies and individual loan underwriting decisions.

Role and Responsibilities of Independent Risk Management

Independent risk management is the second of a bank's three lines of defense. Paragraph II.C.2. of the proposed Guidelines provided that independent risk management should oversee the bank's risk-taking activities and assess risks and issues independent of the CEO and front line units. The proposed Guidelines provided that independent risk management should take primary responsibility and be held accountable by the CEO and board of directors for designing a Framework commensurate with the bank's size, complexity, and risk profile that meets the Guidelines. Paragraph (b) provided that independent risk management should identify and assess, on an ongoing basis, the bank's material aggregate risks and use such risk assessments as the basis for fulfilling its responsibilities under paragraphs (c) and (d) of paragraph II.C.2., and for determining if actions need to be taken to strengthen risk management or reduce risk given changes in the bank's risk profile or other conditions. Paragraph (c) provided that independent risk management should establish and adhere to enterprise policies that include concentration risk limits that ensure that aggregate risks within the bank are effectively identified, measured, monitored, and controlled, consistent with the bank's risk appetite statement and all policies and processes established under paragraphs II.G. through K. Paragraphs (d) and (e) provided that independent risk management should establish and adhere to procedures and processes necessary to ensure compliance with the aforementioned policies and to ensure that the front line units meet the standards discussed in paragraph II.C.1.

Paragraph (f) provided that independent risk management should identify and communicate to the CEO and the board of directors or its risk committee material risks and significant instances where independent risk management's assessment of risk differs

[38] ''Compliance Management System'' booklet of the *Comptroller's Handbook* (Aug. 1996).

[39] *Id.* at 1.

[40] *Id.*

[41] The expectation that banks establish a loan review program are set out in 12 CFR part 30, Appendix A.

from a front line unit as well as significant instances where a front line unit is not complying with the Framework. Paragraph (g) provided that independent risk management should identify and communicate to the board of directors or its risk committee material risks and significant instances where independent risk management's assessment of risk differs from the CEO, and significant instances where the CEO is not adhering to, or holding front line units accountable for adhering to, the Framework. In addition, the proposed Guidelines provided that independent risk management should develop, attract and retain talent, maintain appropriate staffing levels, and establish and adhere to talent management processes and compensation and performance management programs that comply with paragraphs II.L. and II.M., respectively, of the Guidelines.

Commenters proposed several revisions to this section of the proposed Guidelines. Some commenters requested that the OCC delete the provision discussing independent risk management's oversight of the bank's risk-taking activities and assessment of risks and issues independent of the CEO. These commenters expressed concern that this suggested that the CRE would not be subject to CEO oversight with respect to these activities.

Some commenters also noted that including organizational units, such as compliance, legal, and human resources, in the front line unit would require independent risk management to duplicate the control and support functions performed by these other units. These commenters noted that this would detract from independent risk management's responsibilities for overseeing the risk management program. Other commenters requested that the OCC clarify how independent risk management would interact with organizational units performing control functions. For example, some commenters were concerned that independent risk management's oversight function would extend to independently assessing the risks imposed by litigation. As described in the section discussing the front line unit definition, the OCC has made revisions to the definition of front line unit that the OCC believes addresses these concerns.

The OCC is finalizing the role and responsibilities of independent risk management substantially as proposed, with several clarifying changes. The OCC has revised the role and responsibilities of independent risk management to remove the provision that independent risk management should assess risks and issues independent of the CEO. The OCC 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. Notwithstanding the CEO's oversight of the CRE and independent risk management, the OCC emphasizes that paragraph (f) of the final Guidelines continues to provide that independent risk management should report to the board of directors or its risk committee material risks and significant instances where independent risk management's assessment of risk differs from the CEO, as well as significant instances where the CEO is not adhering to, or holding front line units accountable for adhering to, the Framework.

The OCC also emphasizes that the standards articulated in paragraphs (c)[42] and (d) of the final Guidelines should not be interpreted as an exclusive list of actions independent risk management should take to effectively manage risk. Independent risk management should use its risk assessments to determine if additional actions are necessary to strengthen risk management practices or reduce risk. For example, there may be instances where independent risk management should take action to effectively manage risk, even if the covered bank's risk appetite, applicable concentration risk limits, or a front line unit's risk limits have not been exceeded.

The OCC also has removed paragraph (e), and redesignated paragraph (f) as new paragraph (e). The OCC has revised new paragraph (e) to clarify that independent risk management should identify and communicate to the CEO and the board of directors, or the risk committee thereof, significant instances where a front line unit is not adhering to the Framework, including instances when front line units do not meet the standards set forth in paragraph II.C.1.

Role and Responsibilities of Internal Audit

Internal audit is the third of a bank's three lines of defense. The proposed Guidelines provided that internal audit should ensure that a bank's Framework complies with the Guidelines and is appropriate for the bank's size, complexity, and risk profile. Paragraph (a) provided that internal audit should maintain a complete and current inventory of all of the bank's material businesses, product lines, services, and functions and assess the risks associated with each,[43] which collectively provide a basis for the audit plan.

Paragraph (b) provided that internal audit should establish and adhere to an audit plan updated at least quarterly that takes into account the bank's risk profile as well as emerging risks and issues. The proposal provided that the audit plan should require 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. The proposal provided that changes to the audit plan should be communicated to the audit committee of the board of directors.

Paragraph (c) provided that internal audit should report in writing to the audit committee conclusions, issues, and recommendations resulting from the audit work carried out under the audit plan. These reports should identify the root cause of any issue and include a determination of whether the root cause creates an issue that has an impact on one organizational unit or multiple organizational units within the bank, as well as a determination of the effectiveness of front line units and independent risk management in identifying and resolving issues in a timely manner.

Paragraph (d) provided that internal audit should establish and adhere to processes for independently assessing the design and effectiveness of the Framework. The assessment should be performed at least annually and may be conducted by internal audit, an external party, or a combination of both. The assessment should include a conclusion on the bank's compliance with the Guidelines and the degree to which the bank's Framework is consistent with leading industry practices.

Paragraph (e) provided that internal audit should identify and communicate to the audit committee significant instances where front line units or independent risk management are not adhering to the Framework. Paragraph (f) provided that internal audit should establish a quality assurance department

[42] Paragraph (c) provides, in part, that independent risk management should establish and adhere to enterprise policies that include concentration risk limits. Consistent with the proposed Guidelines, a concentration of risk refers to an exposure with the potential to produce losses large enough to threaten a covered bank's financial condition or its ability to maintain its core operations. Risk concentration can arise in a covered bank's assets, liabilities, or off-balance sheet items. An example of a concentration of credit risk limit would be commercial real estate balances as a percentage of capital.

[43] The preamble discussion of this paragraph provided that ''[i]nternal audit should derive the[] [risk] ratings from its Bank-wide risk assessments, and should periodically adjust these ratings based on risk assessments conducted by front line units and changes in the Bank's strategy and the external environment.'' *See* 79 FR 4288.

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 bank, are updated to reflect changes to internal and external risk factors, and are consistently followed. Finally, the proposed Guidelines provided that internal audit should develop, attract, and retain talent and maintain appropriate staffing levels, and establish and adhere to talent management processes and compensation and performance management programs that comply with paragraphs II.L. and II.M., respectively, of the proposed Guidelines.

The OCC invited comment as to whether the final Guidelines should provide that independent risk management maintain a complete and current inventory of all of a bank's material businesses, product lines, services, and functions to ensure that internal audit has developed an accurate inventory. The OCC also requested comment on whether internal audit's assessment of the bank's Framework should include a conclusion regarding whether the Framework is consistent with leading industry practices. The OCC inquired as to whether such an assessment would be possible given the wide range of industry practices, and whether there were any concerns related to this provision.

Commenters generally stated that the role and responsibilities assigned to internal audit were too prescriptive. Some commenters requested that the final Guidelines provide that internal audit report to the audit committee only on *material* changes to the audit plan, *material* audit findings and conclusions, and root causes of *material* audit matters. Other commenters noted that internal audit may not need to assess the Framework's design annually since the design of the Framework is not likely to materially change on a frequent basis. These commenters also expressed concern that the proposed Guidelines could permit an external party to assess the Framework, and requested that the final Guidelines clarify that internal audit must oversee the external party. Some commenters also argued that it is not necessary for internal audit to establish a quality assurance department because this is already a function of internal audit.

Commenters also requested clarification regarding a discussion in the preamble to the proposed Guidelines providing, in part, that the audit plan should rate the risk presented by each front line unit, product line, service, and function, and that internal audit should derive these ratings from bank-wide risk assessments. Some commenters requested clarification regarding whether the bank-wide risk assessments are prepared by internal audit independently, or whether these assessments are prepared by internal audit in conjunction with front line units and/or independent risk management. Other commenters suggested that permitting internal audit to periodically adjust these ratings based on risk assessments conducted by front line units may compromise internal audit's independence and objectivity. Some commenters suggested that internal audit should conduct an independent assessment, and provide challenges where appropriate, to the risk assessments conducted by front line units.

Commenters disagreed whether both independent risk management and internal audit should maintain a complete and current inventory of all of a bank's material businesses, product lines, services, and functions. Some commenters argued that front line units should be responsible for this inventory, rather than internal audit. Other commenters asserted that independent risk management should maintain this inventory rather than internal audit. These commenters noted that internal audit should review and evaluate the inventory for accuracy and completeness if it is maintained by independent risk management. Other commenters expressed the view that banks should have flexibility in determining whether independent risk management or internal audit is responsible for maintaining the inventory. These commenters emphasized that banks should only be required to maintain one comprehensive inventory, and that front line units should play a significant role in the creation of the inventory.

The majority of commenters also opposed the proposed Guidelines to the extent they provided that internal audit's assessment of the bank's Framework should include a conclusion regarding whether the Framework is consistent with leading industry practices. Some commenters noted that this would be a subjective determination as there is no basis for determining what constitutes leading industry practices, and argued that this may lead covered banks to make greater use of third-party consultants. Some commenters also argued that this would detract from internal audit's core functions. Other commenters argued that there are a range of acceptable practices and that it is not possible to establish a single set of leading industry practices. The majority of commenters recommended removing this provision from the final Guidelines.

The OCC's final Guidelines contain revisions to address some of the concerns raised by commenters and to provide internal audit more flexibility in satisfying its role and responsibilities under the Framework. For example, the OCC agrees with commenter suggestions that internal audit should report conclusions and material issues and recommendations to the audit committee pursuant to paragraph (c), and that such reports should also identify the root cause of any material issues. The OCC believes that this modification avoids imposing undue operational burdens on the audit committee and enables the committee to fulfill its key oversight role.

The OCC believes that the design and implementation of the audit plan is an important element of internal audit's role and responsibilities under the Framework. The inventory of material processes, product lines, services, and functions and the risk assessments conducted by internal audit pursuant to paragraph (a) of the final Guidelines is commonly referred to as the ''internal audit universe'' and forms the basis of the audit plan. The OCC expects internal audit to conduct these risk assessments independent of other organizational units in the covered bank. As explained in the preamble to the proposed Guidelines, the audit plan should rate the risk presented by each front line unit, product line, service, and function. This includes activities that the covered bank may outsource to a third party.

Internal audit can leverage risk assessments conducted by front line units or independent risk management in deriving the risk assessments discussed in paragraph (a), but should apply independent judgment in doing so.[44] Internal audit may periodically adjust its risk assessments based on changes in the covered bank's strategy and the external environment. The audit plan should include ongoing monitoring to identify emerging risks and ensure that units, product lines, services, and functions that receive a low risk rating are reevaluated with reasonable frequency.

[44] The OCC does not believe that permitting internal audit to leverage risk assessments conducted by front line units or independent risk management compromises internal audit's independence or objectivity. Specifically, the OCC expects internal audit to report discrepancies in internal audit's risk ratings and a front line unit's or independent risk management's risk ratings to the audit committee of the board of directors.

The audit plan should require 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. The OCC notes that this provision is in addition to internal audit's traditional testing of internal controls and the accuracy of financial records, as required by other laws and regulations at an appropriate frequency based on risk. This testing should require the evaluation of reputation and strategic risk, along with evaluations of independent risk management and traditional risks. This testing should enable internal audit to assess the appropriateness of risk levels and trends across the covered bank.

Consistent with the proposal, the OCC continues to believe that all significant changes to the audit plan should be communicated to the audit committee. As discussed earlier, the OCC believes that the audit plan is a critical element of internal audit's role and responsibilities under the Framework and that significant changes to the audit plan are material. The final Guidelines also clarify that internal audit should periodically review and update the audit plan, rather than performing this task on a quarterly basis as provided in the proposed Guidelines.

Paragraph (c) provides, in part, that internal audit should report in writing, conclusions and material issues and recommendations resulting from audit work carried out under the audit plan. The OCC also notes that these reports should address potential and emerging concerns, the timeliness of corrective actions, and the status of outstanding issues. Finally, audit reports should include comments on the effectiveness of front line units and independent risk management in identifying and mitigating excessive risks and identifying and resolving issues in a timely manner. Audit reports should also reflect emerging risks and internal audit's assessment of the appropriateness of risk levels relative to both the quality of the internal controls and the risk appetite statement.

The OCC has also clarified the role and responsibilities of internal audit under the final Guidelines. Specifically, the final Guidelines provide that internal audit should assess emerging risks and that the quality assurance program should ensure that internal audit's policies, procedures, and processes are updated to reflect emerging risks and improvements in industry internal audit practices. The addition of emerging risks is intended to emphasize that internal audit should consider both pre-existing and prospective risks with respect to the relevant provisions. The OCC also believes that those individuals carrying out the quality assurance program should remain apprised of evolving industry internal audit practices, and that internal audit's policies, procedures, and processes should be updated to reflect these improved practices, as appropriate. The OCC has not removed the provision regarding the establishment of a quality assurance program, as one commenter suggested, because the OCC's supervisory experience indicates that not all covered banks' internal audit units include a quality assurance function.

The OCC has made important revisions to internal audit's role and responsibilities for assessing the design and ongoing effectiveness of the Framework. The final Guidelines continue to provide that this assessment should be conducted at least annually because there may be situations (*e.g.,* expansion of business, change in strategy, emerging risks) that cause the covered bank's risk profile to change, thereby justifying a reassessment of the design and ongoing effectiveness of the covered bank's Framework. The final Guidelines also continue to provide that internal audit, an external party, or both may perform this assessment. The OCC has not revised the final Guidelines to provide that internal audit must oversee this external party. The OCC notes that there may be situations where a covered bank wants to engage a third party to review the entire Framework, including internal audit's role in the Framework. It would not be appropriate for internal audit to oversee the external party in this situation. In addition, based on the overwhelming majority of comments, the OCC is modifying this paragraph to remove the provision that internal audit's assessment of the Framework should include a conclusion regarding whether the Framework is consistent with leading industry practices. However, the OCC notes that most covered banks that experienced difficulties during the financial crisis had risk management practices that were not commensurate with the scope of the covered bank's business activities. As a result, the OCC expects independent risk management, in conjunction with internal audit, the CEO, and the board of directors to assess whether the covered bank's risk management practices are developing in an appropriate manner and consider benchmarking these practices against peers, where possible.

The final Guidelines continue to provide that internal audit should maintain a complete and current inventory (''audit universe'') of all of the covered bank's material processes, product lines, services, and functions. The OCC agrees with commenter suggestions that a covered bank should only be required to maintain one inventory. The OCC believes that internal audit should maintain this inventory, because it is a key component in the creation of the audit plan. Front line units and independent risk management are expected to conduct risk assessments as part of their responsibilities within the Framework and internal audit may use these risk assessments when conducting its risk assessment against the inventory.

Stature

As we noted in the preamble to the proposal, a critical part of an effective Framework is for independent risk management and internal audit to have the organizational stature needed to effectively carry out their respective roles and responsibilities. One of the primary reasons for assigning CRE and CAE responsibilities to individuals who report directly to the CEO is to establish organizational stature for these units. However, evidence of stature extends beyond the reporting structure. Appropriate stature is evidenced by the attitudes and level of support provided by the board of directors, CEO, and others within the covered bank toward these units. The board of directors demonstrates support for these units by ensuring that they have the resources needed to carry out their responsibilities and by relying on the work of these units when carrying out their oversight responsibilities set forth in section III of the final Guidelines. The CEO and front line units demonstrate support by welcoming credible challenges from independent risk management and internal audit and including these units in policy development, new product and service deployment, changes in strategy and tactical plans, and organizational and structural changes.

Strategic Plan

Paragraph D. of section II of the proposed Guidelines provided that the CEO should develop a written strategic plan with input from front line units and independent risk management. The proposal also provided that the board of directors should evaluate and approve the strategic plan and monitor management's efforts to implement it at least annually. Under the proposed Guidelines the strategic plan would cover a three-year period and would contain a comprehensive assessment of risks that currently have an impact on the bank or that could have an impact

on the bank during this period, articulate an overall mission statement and strategic objectives for the bank, and include an explanation of how the bank will achieve those objectives.

The proposal also provided that the strategic plan should include an explanation of how the bank will update the Framework and account for changes in the bank's risk profile projected under the strategic plan. Finally, the proposed Guidelines required the bank to review, update and approve the strategic plan due to changes in the bank's risk profile or operating environment that were not contemplated when the plan was developed.

Some commenters suggested that the CEO should ''oversee'' rather than ''develop'' the strategic plan. Other commenters recommended that the OCC require ''material'' risks to be included in the comprehensive assessment of risks. One commenter suggested that the strategic plan incorporate a capital plan. Some commenters objected to the requirement that the plan include an explanation of how the bank will update the Framework to account for changes in the bank's risk profile. The commenters argued that annual review was sufficient. Another commenter argued that internal audit should not be included in the development of the strategic plan since its involvement could compromise the independence of internal audit.

The OCC is adopting this paragraph substantially as proposed with one minor revision. We have changed the language in the final Guidelines so that a CEO should be ''responsible for the development of,'' rather than ''develop,'' a written strategic plan. This change clarifies that a CEO is not individually expected to prepare the strategic plan. The final Guidelines do not include a materiality threshold for what risks covered banks must assess. While the OCC understands that certain *de minimis* risks may be excluded from the risk assessment, the strategic plan should comprehensively assess all risks that could reasonably be expected to have an impact on the covered bank.

The final Guidelines, like the proposed Guidelines, require a three-year plan. The OCC believes that a three-year plan is necessary for covered banks to predict changes that could affect the bank's financial position. If a covered bank experiences, or expects to experience, significant changes over a three-year time horizon, it must be able to predict and manage the risks associated with those changes. A strategic plan of less than three years would be insufficient to manage longer-term risks to the covered bank. The final Guidelines also do not include a requirement for a specific capital plan. While the OCC acknowledges the importance of capital planning, the final Guidelines are focused on risk management rather than on ensuring adequate capital ratios.

The board of directors should evaluate and approve the strategic plan and monitor management's efforts to implement the strategic plan at least annually. While the OCC expects that for some covered banks an annual review of the Framework may be sufficient, other covered banks that have undergone major changes (for example, mergers) are expected to update their Frameworks to account for changed circumstances. The final Guidelines, like the proposal, provide that the strategic plan should be developed with input from internal audit. The OCC believes that internal audit can contribute to a strategic plan while maintaining the appropriate level of independence.

Risk Appetite Statement

Paragraph E. of section II of the proposed Guidelines provided that the bank should have a comprehensive written statement that articulates a bank's risk appetite and serves as a basis for the Framework (Statement). The term risk appetite means 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 applicable capital, liquidity, and other regulatory requirements.

The proposal noted that the Statement should include: (i) Qualitative components that describe a safe and sound ''risk culture'' [45] and how the bank would assess and accept risks, including those that are difficult to quantify; and (ii) quantitative limits that incorporate sound stress testing processes and, as appropriate, address the bank's earnings, capital and liquidity position. The proposed Guidelines also provided that the bank should set limits at levels that consider appropriate capital and liquidity buffers and prompt management and the board to reduce risk before the bank's risk profile jeopardizes the adequacy of its earnings, liquidity, and capital.[46]

One commenter objected to the language in the preamble to the proposed Guidelines providing that when a bank's risk profile is substantially the same as its parent company, the bank's board may tailor the parent company's risk appetite statement to make it applicable to the bank. According to the commenter, a bank that meets the ''substantially the same'' test should be able to use the same risk appetite statement as its parent company. Another commenter requested clarification on the extent to which a board of directors is required to approve risk limits in connection with a Statement. The commenter argued that bank directors are not in a position to approve all of the limits necessary to manage risk.

The OCC is adopting this paragraph as proposed with only technical changes. As with the proposed Guidelines, the final Guidelines do not include a specific regulatory definition of risk culture. However, setting an appropriate tone at the top is critical to establishing a sound risk culture, and the qualitative statements within the Statement should articulate the core values that the board and CEO expect employees throughout the covered bank to share when carrying out their respective roles and responsibilities within the covered bank. These values should serve as the basis for risk-taking decisions made throughout the covered bank and should be reinforced by the actions of the board, executive management, board committees, and individuals. As noted in the preamble to the proposed Guidelines, evidence of a sound risk culture includes, but is not limited to: (i) Open dialogue and transparent sharing of information between front line units, independent risk management, and internal audit; (ii) consideration of all relevant risks and the views of independent risk management and internal audit in risk-taking decisions; and (iii) compensation and performance management programs and decisions that reward compliance with the core values and quantitative limits established in the Statement, and hold accountable those who do not conduct themselves in a manner consistent with these articulated standards.

As described in paragraph II.E. of the final Guidelines, quantitative limits in a covered bank's Statement should

[45] While there is no regulatory definition of risk culture, for purposes of these Guidelines, risk culture can be considered the shared values, attitudes, competencies, and behaviors present throughout the covered bank that shape and influence governance practices and risk decisions.

[46] The level and types of risk covered bank management and the board of directors are willing to assume to achieve the bank's strategic objectives and business plan should be consistent with its capital and liquidity needs and requirements, as well as other laws and regulatory requirements applicable to the covered bank. The board is not responsible for setting specific risk limits, but the board is required to review and approve the Statement.

incorporate sound stress testing processes, as appropriate, and should address the covered bank's earnings, capital, and liquidity. The covered bank may set quantitative limits on a gross or net basis. Lagging indicators, such as delinquencies, problem asset levels, and losses generally will not capture the build-up of risk during healthy economic periods. As a result, these indicators are generally not useful in proactively managing risk. However, setting quantitative limits based on performance under various adverse scenarios would enable the board and management to take actions that reduce risk before delinquencies, problem assets, and losses reach excessive levels.

We expect examiners to apply judgment when determining which quantitative limits should be based on stress testing and to consider several factors, including, for example, the value in using such measures for the risk type, the covered bank's ability to produce such measures, the capabilities of similarly-situated institutions, and the degree to which the covered bank's board and management have invested in the resources needed to establish such capabilities. We note that the Federal banking agencies issued guidance on stress testing in May 2012.[47] The guidance describes various stress testing approaches and applications, and covered banks should consider the range of approaches and select the one(s) most suitable when establishing quantitative limits. Risk limits may be designed as thresholds, triggers, or hard limits, depending on how the board and management choose to manage risk. Thresholds or triggers that prompt discussion and action before a hard limit is reached or breached can be useful tools for reinforcing risk appetite and proactively responding to elevated risk indicators.

When a covered bank's risk profile is substantially the same as that of its parent company, the covered bank's board may tailor the parent company's risk appetite statement to make it applicable to the covered bank. However, to ensure the sanctity of the national bank or Federal savings association charter, the board of any covered bank must approve the bank-level Statement and document any necessary adjustments or material differences between the covered bank's and parent company's risk profiles.

Concentration and Front Line Unit Risk Limits

Paragraph F. of section II of the proposed Guidelines provided that the Framework should include concentration risk limits and, as applicable, front line unit risk limits for the relevant risks in each front line unit to ensure that these units do not create excessive risks. The proposal also provided that when aggregated across units, these risks do not exceed the limits established in the bank's risk appetite statement.

One commenter suggested that the word ''ensure'' should not be used in this paragraph as it implies a guaranteed outcome. The commenter suggested a slightly different formulation of the language in this paragraph. The OCC is adopting this paragraph as proposed with the addition of the commenter's suggestion. The final Guidelines, state that concentration and front line unit risk limits should limit excessive risk taking.

Risk Appetite Review, Monitoring, and Communication Processes

Paragraph G. of section II of the proposed Guidelines provided that the Framework should require: (i) Review and approval of the Statement by the board or the board's risk committee at least annually or more frequently, as necessary, based on the size and volatility of risks and any material changes in the bank's business model, strategy, risk profile, or market conditions; (ii) initial communication and ongoing reinforcement of the bank's Statement throughout the bank to ensure that all employees align their risk-taking decisions with the Statement; (iii) independent risk management to monitor the bank's risk profile in relation to its risk appetite and compliance with concentration risk limits and to report such monitoring to the board or the board's risk committee at least quarterly; (iv) front line units to monitor their respective risk limits and to report to independent risk management at least quarterly; and (v) when necessary due to the level and type of risk, independent risk management to monitor front line units' compliance with front line unit risk limits, ongoing communication with front line units regarding adherence to these risk limits, and to report any concerns to the CEO and the board or the board's risk committee, at least quarterly.

We received only minor comments on this paragraph and, accordingly, we are adopting paragraph G. of the final Guidelines substantially as proposed, with a few technical changes. With regard to the monitoring and reporting set forth in paragraph G., we note that the frequency of such monitoring and reporting should be performed more often, as necessary, based on the size and volatility of the risks and any material change in the covered bank's business model, strategy, risk profile, or market conditions.

Processes Governing Risk Limit Breaches

Paragraph H. of section II of the proposed Guidelines set out processes governing risk limit breaches. The proposal provided that the bank should establish and adhere to processes that require front line units and independent risk management, in conjunction with their respective responsibilities, to identify any breaches of the Statement, concentration risk limits, and front line unit risk limits, distinguish identified breaches based on the severity of their impact on the bank and establish protocols for when and how to inform the board, front line management, independent risk management, and the OCC of these breaches. The proposed Guidelines also provided that the bank should include in the protocols discussed above the requirement to provide a written description of how a breach will be, or has been, resolved and 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. Under the proposal, while both escalation and resolution processes are important elements of the Framework, it would be acceptable for banks to have different escalation and resolution processes for breaches of the Statement, concentration risk limits, and front line unit risk limits.

The OCC did not receive any comments on this paragraph, and is adopting it as proposed with one change. We have included internal audit in the list of groups that will be informed of a risk limit breach.

Concentration Risk Management

Paragraph I. of section II of the proposed Guidelines provided that the Framework should include policies and supporting processes that are appropriate for the bank's size, complexity, and risk profile that effectively identify, measure, monitor, and control the bank's concentration of risk. The OCC received no comments on this paragraph, and the final Guidelines are adopted as proposed with minor technical changes.

Concentrations of risk can arise in any risk category, with the most common being identified with borrowers, funds providers, and counterparties. In addition, the OCC's eight categories of risk discussed earlier are not mutually

[47] 77 FR 29458 (May 17, 2012).

exclusive; any product or service may expose a covered bank to multiple risks and risks may also be interdependent.[48] Furthermore, concentrations can exist on and off the balance sheet. Covered banks should continually enhance their concentration risk management processes to strengthen their ability to effectively identify, measure, monitor, and control concentrations that arise in all risk categories.[49]

Risk Data Aggregation and Reporting

Paragraph J. of section II of the proposed Guidelines addressed risk data aggregation and reporting. This paragraph provided that the Framework should include a set of policies, supported by appropriate procedures and processes, designed so that the bank's risk data aggregation and reporting capabilities are appropriate for its size, complexity, and risk profile and support supervisory reporting requirements. The proposal provided that these policies, procedures, and processes should collectively provide for the design, implementation, and maintenance of data architecture and information technology infrastructure that support the bank's risk aggregation and reporting needs in times of normalcy and stress; the capturing and aggregating of risk data and reporting of material risks, concentrations, and emerging risks in a timely manner to the board and the OCC and the distribution of risk reports to all relevant parties at a frequency that meets the needs for decision-making purposes.

The OCC is adopting the final Guidelines substantially as proposed with a few technical changes. The OCC expects covered banks to have risk aggregation and reporting capabilities that meet the board's and management's needs for proactively managing risk and ensuring the covered bank's risk profile remains consistent with its risk appetite.

Relationship of Risk Appetite Statement, Concentration Risk Limits, and Front Line Unit Risk Limits to Other Processes

Paragraph K. of section II of the proposed Guidelines addressed the relationship between the Statement, concentration risk limits, and front line unit risk limits to other bank processes. The OCC received no comments on this paragraph and the OCC is adopting this section as proposed with minor technical changes. The covered bank's front line units and independent risk management should incorporate at a minimum the Statement, concentration risk limits, and front line unit risk limits into their strategic and annual operating plans, capital stress testing and planning processes, liquidity stress testing and planning processes, product and service risk management processes (including those for approving new and modified products and services), decisions regarding acquisitions and divestitures, and compensation performance management programs.

Talent Management Processes

The proposed Guidelines provided that the bank should establish and adhere to processes for talent development, recruitment, and succession planning to ensure that management and employees who are responsible for or influence material risk decisions have the knowledge, skills, and abilities to effectively identify, measure, monitor, and control relevant risks. This paragraph also provided that a bank's talent management processes should ensure that the board of directors or a committee of the board: (i) Hires a CEO and approves the hiring of direct reports of the CEO with the skills and abilities to design and implement an effective Framework; (ii) establishes reliable succession plans for the CEO and his or her direct reports; and (iii) oversees the talent development, recruitment, and succession planning processes for individuals two levels down from the CEO. The proposal also provided that these processes should ensure that the board of directors or a committee of the board: (i) hires one or more CREs and a CAE that possess the skills and abilities to effectively implement the Framework; (ii) establishes reliable succession plans for the CRE and CAE; and (iii) oversees the talent development, recruitment, and succession planning processes for independent risk management and internal audit.

Some 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. Commenters noted that the establishment of succession plans for direct reports of the CEO and the oversight of talent development, recruitment, and succession processes for independent risk management, internal audit, and individuals two levels down from the CEO would be burdensome and are more appropriately assigned to bank management. These commenters argued that the OCC should remove these provisions from the final Guidelines.

One commenter noted that it would be sufficient for the board of directors to oversee the talent development, recruitment, and succession planning for individuals one level down from the CEO. Another commenter argued that the OCC should expressly require succession planning for individuals two levels down from the CRE and CAE and require that succession plans identify one or more viable candidates for key positions. Another commenter construed this paragraph as imposing a general requirement that all banks hire dedicated CEOs, CREs, and CAEs, and argued that banks should be permitted to rely on ''dual-hatted'' employees. As previously discussed, the final Guidelines permit a covered bank to use components of its parent company's risk governance framework, including having employees serve in the same position at the covered bank and the parent company, to the extent this is appropriate for the covered bank. The OCC believes that this responds to this commenter's concerns.

In light of the comments received, the OCC has revised this paragraph to reduce the operational burdens on the board of directors while maintaining appropriate board oversight of the talent management program for employees with significant responsibilities under the Framework. The final Guidelines provide that a covered bank's board of directors or an appropriate committee of the board 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 Framework. This provision clarifies that the board of directors need not be involved in the hiring process for these individuals. This gives the board, or a committee thereof, the option to rely on management to appoint the CAE and CRE(s).[50] Similarly, the final Guidelines provide that a covered bank's board of directors or an appropriate committee of the board should review and approve a written talent management program that provides for development, recruitment, and succession planning regarding the CEO, CAE, CRE(s), their direct reports, and other potential successors. The OCC

[48] *See* ''Large Bank Supervision'' booklet of the *Comptroller's Handbook* (Jan. 2010).

[49] *See* ''Concentrations of Credit'' booklet of the *Comptroller's Handbook* (Dec. 2011); Interagency Supervisory Guidance on Counterparty Credit Risk Management at *http://www.occ.gov/news-issuances/bulletins/2011/bulletin-2011-30.html.*

[50] The OCC notes that the definition of ''independent risk management'' provides that the board of directors or its risk committee should approve all decisions regarding the appointment or removal of a CRE, while the definition of ''internal audit'' provides that the audit committee should approve all decisions regarding the appointment or removal of the CAE. *See* final Guidelines paragraphs I.E.7. and 8.

believes that this revision reduces the talent management responsibilities of the board of directors, or a committee thereof, because they are no longer expected to oversee the talent development, recruitment, and succession planning processes for independent risk management, internal audit, and individuals two levels down from the CEO, as provided in the proposed Guidelines. Instead, the board of directors, or a committee thereof, should review and approve a written talent management program for key employees in a covered bank's Framework. The OCC notes that it is very important that covered banks detail the development, recruitment, and succession planning for these individuals because they occupy critical positions in a covered bank's Framework.

Finally, the final Guidelines provide that a covered bank's board of directors or an appropriate committee of the board should require management to assign individuals specific responsibilities within the talent management program, and hold those individuals accountable for the program's effectiveness. This provision clarifies that the OCC expects the board of directors, or a committee thereof, to provide oversight to a covered bank's talent management program, and that responsibility for developing and implementing this program rests with covered bank management.

Compensation and Performance Management Programs

The proposed Guidelines provided that a bank should establish and adhere to compensation and performance management programs that meet the requirements of any applicable statute or regulation. The proposal provided that these programs should be appropriate to ensure that the CEO, front line units, independent risk management, and internal audit implement and adhere to an effective Framework. The proposal also provided that programs should ensure that front line unit compensation plans and decisions appropriately consider the level and severity of issues and concerns identified by independent risk management and internal audit. The programs should be designed to attract and retain the talent needed to design, implement, and maintain an effective Framework. Finally, the proposed Guidelines provided that the programs should prohibit incentive-based payment arrangements, or any feature of any such arrangement, that encourages inappropriate risks by providing excessive compensation or that could lead to material financial loss.

Some commenters supported this paragraph of the proposed Guidelines. One commenter argued that employee compensation should be linked to the entire organization's strategic goals and should incorporate organization-wide performance metrics. Another commenter requested that the OCC provide more specific standards for compensation. A commenter also objected to the proposed Guidelines to the extent they provided that the programs should ensure front line unit compensation plans and decisions appropriately consider the level and severity of issues, and instead suggested that the Guidelines should emphasize the timely correction of issues.

Commenters also disagreed regarding the inclusion of the incentive compensation provision in the proposed Guidelines. Some commenters suggested that the proposed Guidelines should contain stronger language prohibiting incentive-based payment arrangements that encourage inappropriate risk. Other commenters argued that one could interpret this provision as creating standards beyond those established by existing interagency guidance as well as those set out in joint agency proposed rulemaking. These commenters recommended revising this provision to state that a bank's compensation and performance management programs should meet the requirements of applicable laws and regulations.

After reviewing the comments received, the OCC is adopting the compensation and performance management program paragraph substantially as proposed with clarifying and technical changes. The OCC has revised this paragraph to provide that the compensation and performance management programs should ensure front line unit compensation plans and decisions appropriately consider the level and severity of issues and concerns identified by independent risk management and internal audit, as well as the timeliness of corrective action to resolve such issues and concerns. The OCC declines to remove the term ''severity,'' as suggested by one commenter because we believe this is an important factor in determining the materiality of issues and concerns.

The OCC also has decided not to modify the remaining provisions of this paragraph, including the incentive compensation standard. As previously discussed, the final Guidelines establish minimum standards for the design and implementation of a covered bank's Framework and minimum standards for the covered bank's board of directors in providing oversight to the Framework's design and implementation. While compensation practices are an important part of a covered bank's Framework, the OCC notes that other authorities address this issue in more detail.[51] The OCC reminds covered banks that employee compensation arrangements should comply with all applicable rules and guidance. The OCC also notes that section 956 of the Dodd-Frank Act[52] requires the OCC, the Board, the FDIC, the National Credit Union Administration, the Securities and Exchange Commission, and the Federal Housing Finance Agency to jointly prescribe incentive-based regulations or guidelines applicable to covered institutions.[53] The OCC notes that the incentive compensation standard included in the final Guidelines was adapted from the standard set out in section 956 of the Dodd-Frank Act, and that a covered bank's compensation and performance management programs should comply with the final regulations or guidelines implementing section 956 when they are issued.

Section III: Standards for Board of Directors

Section III of the final Guidelines sets forth the minimum standards for a covered bank's board of directors in providing oversight to the Framework's design and implementation.

Some commenters expressed concern regarding the standards contained in section III of the proposed Guidelines. For example, some commenters argued that the proposed Guidelines would distract the board of directors from its strategic and oversight role. Other commenters asserted that the proposed Guidelines would place an undue burden on the board of directors by assigning managerial responsibilities to the board that are more properly the role

[51] *See* 12 U.S.C. 1831p–1(c); 12 CFR part 30, Appendix A (requiring institutions to maintain safeguards to prevent the payment of compensation, fees, and benefits that are excessive or that could lead to material financial loss to an institution, and prohibiting excessive compensation as an unsafe and unsound practice). As provided in the Guidelines, covered banks subject to the final Guidelines should ensure that practices established within their Frameworks also meet the standards set forth in appendices A, B, and C to part 30. *See* final Guidelines II.C. note 2. We also note that the OCC, Board, the Federal Deposit Insurance Corporation (FDIC), and the OTS issued interagency guidance that addresses incentive-based compensation. *See Guidance on Sound Incentive Compensation Policies,* 75 FR 36395 (June 25, 2010).

[52] 12 U.S.C. 5641.

[53] *See* 76 FR 21170 (Apr. 14, 2011).

of bank management. Some commenters also argued that the oversight mandated by the proposed Guidelines would increase a board of directors' exposure to liability and discourage qualified individuals from agreeing to serve on the board.

The OCC has revised the standards to recognize the board of directors' key strategic and oversight role with respect to the design and implementation of the Framework. The OCC believes that these revisions respond to commenters' concerns and avoid imposing an undue operational burden on the board of directors. Set forth below is a discussion of the minimum standards for a covered bank's board of directors in providing oversight to the Framework's design and implementation under the final Guidelines.

Require an Effective Risk Governance Framework

Paragraph A. of section III of the proposed Guidelines provided that each member of the bank's board of directors has a duty to oversee the bank's compliance with safe and sound banking practices. The proposed Guidelines also provided that the board of directors should ensure that the bank establishes and implements an effective Framework that complies with the Guidelines. Finally, the proposed Guidelines provided that the board of directors or its risk committee should approve any changes to the Framework.

Many commenters strongly opposed the use of the word ''ensure'' in the proposed Guidelines. Some commenters noted that the term ''ensure'' could be read as a guarantee of results and understood to imply that the board of directors is required to be involved in the day-to-day activities of the bank. These commenters asserted that it may make it more difficult for banks to attract qualified candidates for a bank's board of directors and may imply that the board could be held liable for management actions even when director oversight has been reasonable. Other commenters suggested that the final Guidelines should provide that a board of directors fulfills its oversight function by reviewing, evaluating, and approving a Framework that is designed, recommended, and implemented by management and by receiving reports on material compliance matters.

Many commenters recommended that the OCC remove the word ''ensure'' from the final Guidelines, and provided a number of alternatives to address their concerns. Commenters suggested that the OCC replace ''ensure'' with: ''Require,'' ''oversee,'' ''actively oversee,'' and ''oversee and confirm.'' Commenters generally argued that these alternatives more accurately reflect the board of directors' oversight function.

After reviewing the comments, the OCC is revising this paragraph of the final Guidelines to remove the terms ''duty'' and ''ensure.'' The OCC did not intend to impose managerial responsibilities on the board of directors, or suggest that the board must guarantee results under the Framework. Accordingly, consistent with commenter suggestions, the final Guidelines provide that the board of directors should require management to establish and implement an effective Framework that meets the minimum standards described in the Guidelines. The OCC believes that this revision aligns the board of directors' responsibilities under this paragraph with their traditional strategic and oversight role.

The OCC has also modified this paragraph to reduce the operational burdens placed on the board of directors while maintaining their involvement in overseeing the Framework's design and implementation. The final Guidelines clarify that the board of directors or its risk committee should approve significant changes to the Framework and monitor compliance with the Framework. This revision clarifies that the board or risk committee should only approve significant changes to the Framework, rather than all changes, as provided in the proposed Guidelines. This change also clarifies that the board of directors or the risk committee should monitor compliance with the Framework. The board of directors or the risk committee monitors compliance with the Framework by overseeing management's implementation of the Framework and holding management accountable for fulfilling their responsibilities under the Framework.

Provide Active Oversight of Management

Paragraph B. of section III of the proposed Guidelines provided that the board of directors should actively oversee the bank's risk-taking activities and hold management accountable for adhering to the Framework. The proposed Guidelines also provided that the board of directors should question, challenge, and, when necessary, oppose management's proposed actions that could cause the bank's risk profile to exceed its risk appetite or threaten the bank's safety and soundness.

Commenters expressed concern that these provisions would promote confrontation between the board of directors and bank management at board meetings. Some commenters argued that this would deter open and candid dialogue between the board of directors and bank management, and that emphasizing board opposition will detract from determining how active the board is in overseeing management actions.

Some commenters also argued that the board of directors' oversight of management should not be characterized as ''active'' because it implies that board members are implementing and assuming management functions.

The final Guidelines continue to provide that a covered bank's board of directors should *actively oversee* the covered bank's risk-taking activities and hold management accountable for adhering to the Framework. The OCC believes that it is important for the board of directors to understand a covered bank's risk-taking activities and to be engaged in providing oversight to these activities. The final Guidelines clarify that the board of directors provides active oversight by relying on risk assessments and reports prepared by independent risk management and internal audit. Therefore, the final Guidelines do not contemplate that the board of directors will assume managerial responsibilities in providing active oversight of management—instead, the board is permitted to rely on independent risk management and internal audit to meet its responsibilities under this paragraph. Some boards of directors periodically engage third-party experts to assist them in understanding risks and issues and to make recommendations to strengthen board and bank practices. While the Guidelines focus on independent risk management and internal audit, they do not prohibit boards of directors from engaging third-party experts to also assist them in carrying out their duties.

The final Guidelines continue to articulate the OCC's expectation that the board of directors should provide a credible challenge to management. The OCC believes that a board of directors will be able to provide this challenge if its members have a comprehensive understanding of the covered bank's risk-taking activities. During the financial crisis, the OCC observed that some members of the board of directors at certain institutions had an incomplete understanding of their institution's risk exposures. The OCC believes that this evidences both a failure to exercise adequate oversight of management and critically evaluate management's recommendations and decisions during the years preceding the financial crisis.

The OCC believes that the capacity to dedicate sufficient time and energy in

reviewing information and developing an understanding of the key issues related to a covered bank's risk-taking activities is a critical prerequisite to being an effective director. Informed directors are well-positioned to engage in substantive discussions with management wherein the board of directors provides approval to management, requests guidance to clarify areas of uncertainty, and prudently questions the propriety of strategic initiatives. Therefore, the final Guidelines continue to provide that the board of directors, in reliance on information it receives from independent risk management and internal audit, should question, challenge, and when necessary, oppose recommendations and decisions made by management that could cause the covered bank's risk profile to exceed its risk appetite or jeopardize the safety and soundness of the covered bank. In addition to resulting in a more informed board of directors, the OCC expects that this provision will enable the board to make a determination as to whether management is adhering to, and understands, the Framework. For example, recurring breaches of risk limits or actions that cause the covered bank's risk profile to materially exceed its risk appetite may demonstrate that management does not understand or is not adhering to the Framework. In these situations, the board of directors should take action to hold the appropriate party, or parties, accountable.

The OCC does not intend this standard to become a compliance exercise for the covered bank, or lead to scripted meetings between the board of directors and management. Instead, the OCC intends to assess compliance with this standard primarily by engaging OCC examiners in frequent conversations with directors. Likewise, the OCC does not expect the board of directors to evidence opposition to management during each board meeting. Instead, the OCC emphasizes that the board of directors should oppose management's recommendations and decisions only when necessary. The OCC believes that an environment in which examiners, board members, and management openly and honestly communicate benefits a covered bank, and expects these types of interactions to continue.

Exercise Independent Judgment

The proposed Guidelines provided that in carrying out his or her duty to provide active oversight of bank management, a director should exercise sound, independent judgment. We received no comments on this paragraph and adopt it in the final Guidelines substantially as proposed. In determining whether a board member is adequately objective and independent, the OCC will consider the degree to which the member's other responsibilities conflict with his or her ability to act in the covered bank's interest.

Include Independent Directors

Paragraph D. of section III of the proposed Guidelines provided that at least two members of a bank's board of directors should be independent, *i.e.,* they should not be members of the bank's or the parent company's management. In the preamble to the proposal, we noted that this would enable the bank's board to provide effective, independent oversight of bank management and, to the extent the bank's independent directors are also members of the parent company's board, the OCC would expect that such directors would consider the safety and soundness of the bank in decisions made by the parent company that impact the bank's risk profile. The proposal also provided that this standard would not supersede other applicable regulatory requirements concerning the composition of a Federal savings association's board [54] and that these associations must continue to comply with such requirements.

We received a number of comments on this paragraph. Some commenters opposed the requirement for two independent directors. These commenters believe that the bank should have the flexibility to decide the structure of their own board based on their individual business requirements as long as the board appropriately controls risk. One commenter suggested that the requirement for two independent directors not apply to banks with boards with seven or fewer total directors or if the bank can demonstrate that it would be an undue hardship to find two independent directors. A few commenters noted that it would be better to require a percentage of independent directors rather than requiring a specific number. Other commenters supported this requirement.

One commenter noted that our independence standard differed from the Board's standard in their Dodd-Frank Act section 165 rules and suggested that the OCC adopt the Board's standard of independence to be consistent.

The OCC is retaining the requirement for covered banks to have at least two independent board members. However, as suggested by one commenter, we have revised this provision to be consistent with the Board's independence standard in its Dodd-Frank Act section 165 rules.[55] The final Guidelines provide that at least two members of the board of each covered bank should not be an officer or employee of the parent company or covered bank and has not been an officer or employee of the parent company or covered bank during the previous three years; should not be a member of the immediate family, as defined in the Board's Regulation Y,[56] of a person who is, or has been within the last three years, an executive officer of the parent company or covered bank, as defined in the Board's Regulation O; [57] and should qualify as an independent director under the listing standards of a national securities exchange, as demonstrated to the satisfaction of the OCC.

Provide Ongoing Training to Directors

Paragraph E. of section III of the proposed Guidelines provided that in order to ensure that each member of the board of directors has the knowledge, skills, and abilities needed to meet the standards set forth in the Guidelines, the board should establish and adhere to a formal, ongoing training program for directors. The proposed Guidelines provided that the training program apply only to independent directors and should include training on: (i) Complex products, services, lines of business, and risks that have a significant impact on the bank; (ii) laws, regulations, and supervisory requirements applicable to the bank; and (iii) other topics identified by the board of directors.

Some commenters requested that the OCC reconsider this paragraph, and suggested that it may discourage qualified individuals from serving as bank directors. Other commenters recommended that the board of directors should retain discretion in directing the frequency, scope, and selecting the provider of training to

[54] *See* 12 CFR 163.33.

[55] Several commenters also suggested that the OCC coordinate with the Board to ensure that these Guidelines are consistent with the Board's enhanced prudential standards relating to risk management that were issued under section 165 of the Dodd-Frank Act. *See* 12 U.S.C. 5365. The Board's enhanced prudential standards apply to a covered bank's holding company and commenters raised concerns that inconsistencies could create unnecessary burden. We note that OCC staff met with Board staff to discuss the relationship between these Guidelines and the Board's section 165 rules. The independence standard for directors in the final Guidelines is an example of the OCC's efforts to address potential inconsistencies.

[56] 12 CFR 225.41(b)(3).

[57] 12 CFR 215.2(e)(1).

board members. These commenters also suggested that the training program should only include training on material laws, regulations, and supervisory requirements, and that the final Guidelines should permit banks to choose training suited to their business model, risk profile, and the background of board members. Another commenter suggested that the OCC revise this paragraph to enable a bank's independent risk management and/or internal audit units to recommend training to the board of directors.

After considering the comments, the OCC has revised this paragraph in the final Guidelines to apply to all directors [58] but to provide more flexibility to the board of directors in structuring a formal, ongoing training program for directors. Specifically, the final Guidelines incorporate commenters' suggestions and provide that the training program should consider the directors' knowledge and experience and the covered bank's risk profile. This revision reflects the OCC's belief that the training program should be tailored to the director's needs, experience, and education. Similarly, the final Guidelines provide more flexibility to covered banks to focus the training program on material topics because the final Guidelines emphasize that the program should include training on ''appropriate'' areas. The OCC also notes that covered banks retain discretion in directing the frequency, scope, and selecting the provider of training under the final Guidelines.

The OCC continues to believe that the board of directors should be financially knowledgeable and committed to conducting diligent reviews of the covered bank's management team, financial status, and business plans. OCC examiners will evaluate each director's knowledge and experience, as demonstrated in their written biography and discussions with examiners.

Self-Assessments

Paragraph F. of section III of the proposed Guidelines provided that the bank's board of directors should conduct an annual self-assessment that includes an evaluation of the board's effectiveness in meeting the standards provided in section III of the Guidelines.

The OCC received no comments and is adopting this paragraph as proposed. The OCC notes that the self-assessment discussed in this paragraph can be part of a broader self-assessment process conducted by the board of directors, and should result in a constructive dialogue among board members that identifies opportunities for improvement and leads to specific changes that are capable of being tracked, measured, and evaluated. For example, these may include broad changes that range from changing the board of directors' 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.

Relationship Between the Guidelines and OCC's Heightened Expectations Program

As discussed above, the final Guidelines will supersede the current heightened expectations program. The informal guidance communicated in a Deputy Comptroller memo and ''one page'' documents will no longer be used to evaluate covered banks. Examiners will assess covered bank governance and risk management practices using these final Guidelines and other existing OCC policy guidance such as handbooks and bulletins to identify appropriate practices and weaknesses and communicate areas needing improvement to the board of directors and management of covered banks according to existing supervisory processes as described in the ''Bank Supervision Processes'' booklet of the *Comptroller's Handbook.*

Integration of Federal Savings Associations Into Part 30

As noted above, 12 CFR parts 30 and 170 establish safety and soundness rules and guidelines for national banks and Federal savings associations, respectively. The OCC proposed to make part 30 and its respective appendices applicable to both national banks and Federal savings associations. The OCC also proposed to remove part 170, as it would no longer be necessary, and to make other minor changes to part 30, including the deletion of references to rescinded OTS guidance. We received no comments on these amendments and therefore adopt them as proposed, with minor technical drafting corrections. These amendments are described below.

Safety and Soundness Rules. On July 10, 1995, the Federal banking agencies adopted a final rule establishing deadlines for submission and review of safety and soundness compliance plans.[59] The final rule provides that the agencies may require compliance plans to be filed by an insured depository institution for failure to meet the safety and soundness standards prescribed by guideline pursuant to section 39 of the FDIA. The safety and soundness rules for national banks and Federal savings associations are set forth at 12 CFR parts 30 and 170, respectively, and, with one exception discussed below, they are substantively the same.

Twelve CFR part 30 establishes the procedures a national bank must follow if the OCC determines that the bank has failed to satisfy a safety and soundness standard or if the OCC requests the bank to file a compliance plan. Section 30.4(d) provides that if a bank fails to submit an acceptable compliance plan within the time specified by the OCC or fails in any material respect to implement a compliance plan, then the OCC *shall* require the bank to take certain actions to correct the deficiency. However, if a bank has experienced ''extraordinary growth'' during the previous 18-month period, then the rule provides that the OCC *may* be required to take certain action to correct the deficiency. Section 30.4(d)(2) defines ''extraordinary growth'' as ''an increase in assets of more than 7.5 percent during any quarter within the 18-month period preceding the issuance of a request for submission of a compliance plan.''

Twelve CFR part 170 sets forth nearly identical safety and soundness rules for Federal savings associations to those applicable in part 30. However, in contrast to part 30, part 170 does not define ''extraordinary growth.'' Instead, the OCC determines whether a savings association has undergone extraordinary growth on a case-by-case basis by considering various factors such as the association's management, asset quality, capital adequacy, interest rate risk profile, and operating controls and procedures.[60]

In order to streamline and consolidate the safety and soundness rules applicable to national banks and Federal savings associations, the OCC is applying part 30 to Federal savings associations. This change will not subject Federal savings associations to any new requirements but will subject them to the section 30.4(d)(2) definition of ''extraordinary growth.'' This definition incorporates an objective standard for determining ''extraordinary growth'' that is based on an increase in assets over a period of time and will provide greater clarity and guidance to Federal savings associations on when

[58] This provision applies to all directors because directors that are members of management may not have expertise in all matters for which the board of directors may be providing oversight.

[59] *See* 60 FR 35674.

[60] *See* Thrift Regulatory Bulletin 3b, ''Policy Statement on Growth for Savings Associations'' (Nov. 26, 1996).

the OCC would be required to take action to correct a deficiency.

Guidelines Establishing Standards for Safety and Soundness. In conjunction with the final rule establishing deadlines for compliance plans, the agencies jointly adopted Interagency Guidelines Establishing Standards for Safety and Soundness (Safety and Soundness Guidelines) as Appendix A to each of the agencies' respective safety and soundness rules. The Safety and Soundness Guidelines are set forth in Appendix A to parts 30 and 170 for national banks and savings associations, respectively. The texts of Appendix A for national banks and savings associations are substantively identical. Pursuant to section 39 of the FDIA, by adopting the safety and soundness standards as guidelines, the OCC may pursue the course of action that it determines to be most appropriate, taking into consideration the circumstances of a national bank's noncompliance with one or more standards, as well as the bank's self-corrective and remedial responses.

In order to streamline and consolidate all safety and soundness guidelines in one place, this final rule amends Appendix A to part 30 so that it also applies to Federal savings associations. This change will not result in any new requirements for Federal savings associations.

Guidelines Establishing Information Security Standards. Section 501 of the Gramm-Leach-Bliley Act requires the Federal banking agencies, the National Credit Union Administration, the Securities and Exchange Commission, and the Federal Trade Commission to establish appropriate standards relating to administrative, technical, and physical safeguards for customer records and information for the financial institutions subject to their respective jurisdictions. Section 505(b) requires the agencies to implement these standards in the same manner, to the extent practicable, as the standards prescribed pursuant to section 39(a) of the FDIA. Guidelines implementing the requirements of section 501, Interagency Guidelines Establishing Information Security Standards, are set forth in Appendix B to parts 30 and 170 for national banks and Federal savings associations, respectively.[61] The texts of Appendix B for national banks and savings associations are substantively identical.

In order to streamline and consolidate all safety and soundness guidelines in one place, the OCC is amending Appendix B to part 30 so that it also applies to Federal savings associations. This change will not result in any new requirements for Federal savings associations.

Guidelines Establishing Standards for Residential Mortgage Lending Practices. On February 7, 2005, the OCC adopted guidelines establishing standards for residential mortgage lending practices for national banks and their operating subsidiaries as Appendix C to part 30.[62] These guidelines address certain residential mortgage lending practices that are contrary to safe and sound banking practices, may be conducive to predatory, abusive, unfair or deceptive lending practices, and may warrant a heightened degree of care by lenders.

While there is no equivalent to Appendix C in part 170, Federal savings associations are subject to guidance on residential mortgage lending.[63] For many of the same reasons that the OCC decided to incorporate its residential mortgage lending guidance into a single set of guidelines adopted pursuant to section 39, the OCC is now applying Appendix C to Federal savings associations. As a result, Federal savings associations will be subject to the same guidance on residential mortgage lending as national banks, thereby harmonizing residential mortgage lending standards for both types of institutions. Moreover, the application of Appendix C to Federal savings associations clarifies the residential mortgage lending standards applicable to these institutions and enhances the overall safety and soundness of Federal savings associations, because the Appendix C guidelines are enforceable pursuant to the FDIA section 39 process as implemented by part 30. It should be noted, however, that although the guidelines in Appendix C incorporate and implement some of the principles set forth in current Federal savings association guidance on residential real estate lending, they do not replace such guidance.

Description of Technical Amendments to Part 30

We also are including in this final rule technical and conforming amendments to the part 30 regulations to add references to new Appendix D, which contains the Guidelines, where appropriate.

The Guidelines are enforceable, pursuant to section 39 of the FDIA and part 30, as we have described. That enforcement mechanism is not necessarily exclusive, however. Nothing in the Guidelines in any way limits the authority of the OCC to address unsafe or unsound practices or conditions or other violations of law. Thus, for example, a bank's failure to comply with the standards set forth in these Guidelines may also be actionable under section 8 of the FDIA if the failure constitutes an unsafe or unsound practice.

In addition, we are replacing the cross-references to 12 CFR 40.3, the OCC's former privacy rule, with the appropriate cite to the Consumer Financial Protection Bureau's (CFPB) privacy rule, 12 CFR 1016.3, in the definitions of ''customer'' and ''customer information'' in Appendix B to part 30. The Dodd-Frank Act transferred to the CFPB Federal rulemaking authority to issue privacy rules applicable to national banks, as well as Federal savings associations. As a result, 12 CFR part 40 is no longer operative and national banks now must comply with these rules as reissued by the CFPB.[64]

Lastly, in 12 CFR 168.5, we have replaced the reference to part 170 with part 30 to reflect the fact that this final rule removes part 170 and applies part 30 and its appendices to Federal savings associations.

Regulatory Analysis

Paperwork Reduction Act

The OCC has determined that the final Guidelines involve information collection requirements pursuant to the provisions of the Paperwork Reduction Act of 1995 (the PRA) (44 U.S.C. 3501 *et seq.*).

The OCC may not conduct or sponsor, and an organization is not required to respond to, these information collection requirements unless the information collection displays a currently valid Office of Management and Budget (OMB) control number. The OCC has submitted this collection to OMB pursuant to section 3507(d) of the PRA

[61] Appendix B to part 30 currently applies to national banks, Federal branches and agencies of foreign banks, and any subsidiaries of such entities (except brokers, dealers, persons providing insurance, investment companies, and investment advisers).

[62] *See* 70 FR 6329. Appendix C currently applies to national banks, Federal branches and agencies of foreign banks, and any operating subsidiaries of such entities (except brokers, dealers, persons providing insurance, investment companies, and investment advisers).

[63] *See* Examination Handbook Section 212, ''One-to Four-Family Residential Real Estate Lending'' (Feb. 10, 2011) (incorporating Regulatory Bulletin 37–18 (Mar. 31, 2007)) and OCC Bulletin 1999–38, ''Treatment of High LTV Residential Real Estate Loans'' (Oct. 13, 1999).

[64] The OCC removed 12 CFR part 40 from the Code of Federal Regulations earlier this year. 79 FR 15639 (Mar. 21, 2014).

and section 1320.11 of OMB's implementing regulations (5 CFR part 1320).

The OCC submitted this collection to OMB at the proposed rule stage as well. OMB filed comments instructing the OCC to examine public comment in response to the proposed rule and describe in the supporting statement of its next collection any public comments received regarding the collection as well as why (or why it did not) incorporate the commenter's recommendation. The OCC received no comments regarding the collection.

Abstract

The information collection requirements are found in 12 CFR part 30, Appendix D, which establishes minimum standards for the design and implementation of a risk governance framework for insured national banks, insured Federal savings associations, and insured Federal branches of a foreign bank with average total consolidated assets equal to or greater than $50 billion. Insured national banks and insured Federal savings associations with average total consolidated assets of less than $50 billion will also be subject to the Guidelines if that institution's parent company controls at least one insured national bank or insured Federal savings association with average total consolidated assets equal to or greater than $50 billion. The OCC reserves the authority to apply these requirements to an insured national bank, insured Federal savings association, or insured Federal branch of a foreign bank that has average total consolidated assets of less than $50 billion if the OCC determines that its operations are highly complex or otherwise present a heightened risk.

Standards for Risk Governance Framework

Covered banks should establish and adhere to a formal, written risk governance framework designed by independent risk management. It should include delegations of authority from the board of directors to management committees and executive officers as well as risk limits established for material activities. It should be approved by the board of directors or the board's risk committee and reviewed and updated at least annually by independent risk management.

Front Line Units

Front line units should take responsibility and be held accountable by the CEO and the board of directors for appropriately assessing and effectively managing all of the risks associated with their activities. In fulfilling this responsibility, each front line unit should, either alone or in conjunction with another organizational unit that has the purpose of assisting a front line unit: (i) Assess, on an ongoing basis, the material risks associated with its activities and use such risk assessments as the basis for fulfilling its responsibilities and for determining if actions need to be taken to strengthen risk management or reduce risk given changes in the unit's risk profile or other conditions; (ii) establish and adhere to a set of written policies that include front line unit risk limits. Such policies should ensure risks associated with the front line unit's activities are effectively identified, measured, monitored, and controlled, consistent with the covered bank's risk appetite statement, concentration risk limits, and all policies established within the risk governance framework; (iii) establish and adhere to procedures and processes, as necessary to maintain compliance with the policies described in (ii); (iv) adhere to all applicable policies, procedures, and processes established by independent risk management; (v) develop, attract, and retain talent and maintain staffing levels required to carry out the unit's role and responsibilities effectively; (vi) establish and adhere to talent management processes; and (vii) establish and adhere to compensation and performance management programs.

Independent Risk Management

Independent risk management should oversee the covered bank's risk-taking activities and assess risks and issues independent of the front line units by: (i) Designing a comprehensive written risk governance framework commensurate with the size, complexity, and risk profile of the covered bank; (ii) identifying and assessing, on an ongoing basis, the covered bank's material aggregate risks; (iii) establishing and adhering to enterprise policies that include concentration risk limits; (iv) establishing and adhering to procedures and processes, to ensure compliance with policies in (iii); (v) identifying and communicating to the CEO and board of directors or board's risk committee material risks and significant instances where independent risk management's assessment of risk differs from that of a front line unit, and significant instances where a front line unit is not adhering to the risk governance framework; (vi) identifying and communicating to the board of directors or the board's risk committee material risks and significant instances where independent risk management's assessment of risk differs from the CEO, and significant instances where the CEO is not adhering to, or holding front line units accountable for adhering to, the risk governance framework; and (vii) developing, attracting, and retaining talent and maintaining staffing levels required to carry out the unit's role and responsibilities effectively while establishing and adhering to talent management processes and compensation and performance management programs.

Internal Audit

Internal audit should ensure that the covered bank's risk management framework complies with the Guidelines and is appropriate for the size, complexity, and risk profile of the covered bank. It should maintain a complete and current inventory of all of the covered bank's material processes, product lines, services, and functions, and assess the risks, including emerging risks, associated with each, which collectively provide a basis for the audit plan. It should establish and adhere to an audit plan, which is periodically reviewed and updated, that takes into account the covered bank's risk profile, emerging risks, issues, and establishes the frequency with which activities should be audited. The audit plan should require 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 risk governance framework. Significant changes to the audit plan should be communicated to the board's audit committee. Internal audit should report in writing, conclusions and material issues and recommendations from audit work carried out under the audit plan to the board's audit committee. Reports should identify the root cause of any material issue and include: (i) 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 bank; and (ii) a determination of the effectiveness of front line units and independent risk management in identifying and resolving issues in a timely manner. Internal audit should establish and adhere to processes for independently assessing the design and ongoing effectiveness of the risk governance framework on at least an annual basis. The independent assessment should include a conclusion on the covered bank's compliance with the standards set forth in the Guidelines. Internal audit should

identify and communicate to the board of directors or board's audit committee significant instances where front line units or independent risk management are not adhering to the risk governance framework. Internal audit should establish a quality assurance program 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 bank, are updated to reflect changes to internal and external risk factors, emerging risks, and improvements in industry internal audit practices, and are consistently followed. Internal audit should develop, attract, and retain talent and maintain staffing levels required to effectively carry out its role and responsibilities. Internal audit should establish and adhere to talent management processes. Internal audit should establish and adhere to compensation and performance management programs.

Strategic Plan

The CEO, with input from front line units, independent risk management, and internal audit, should be responsible for the development of a written strategic plan that should cover, at a minimum, a three-year period. The board of directors should evaluate and approve the plan and monitor management's efforts to implement the strategic plan at least annually. The plan should include a comprehensive assessment of risks of the covered bank, an overall mission statement and strategic objectives, an explanation of how the covered bank will update the risk governance framework to account for projected changes to its risk profile, and be reviewed, updated, and approved pursuant to changes in the covered bank's risk profile or operating environment that were not contemplated when the plan was developed.

Risk Appetite Statement

A covered bank should have a comprehensive written statement outlining its risk appetite that serves as the basis for the risk governance framework. It should contain qualitative components that define a safe and sound risk culture and how the covered bank will assess and accept risks and quantitative limits that include sound stress testing processes and address earnings, capital, and liquidity.

Risk Limit Breaches

A covered bank should establish and adhere to processes that require front line units and independent risk management to: (i) Identify breaches of the risk appetite statement, concentration risk limits, and front line unit risk limits; (ii) distinguish breaches based on the severity of their impact; (iii) establish protocols for disseminating information regarding a breach; (iv) provide a written description of the breach resolution; and (v) establish accountability for reporting and resolving breaches.

Concentration Risk Management

The risk management framework should include policies and supporting processes appropriate for the covered bank's size, complexity, and risk profile for effectively identifying, measuring, monitoring, and controlling the covered bank's concentrations of risk.

Risk Data Aggregation and Reporting

This risk governance framework should include a set of policies, supported by appropriate procedures and processes, designed to provide risk data aggregation and reporting capabilities appropriate for the covered bank's 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 bank's risk aggregation and reporting needs during normal times and during times of stress; (ii) the capturing and aggregating of risk data and reporting of material risks, concentrations, and emerging risks in a timely manner to the board of directors and the OCC; and (iii) the distribution of risk reports to all relevant parties at a frequency that meets their needs for decision-making purposes.

Talent Management and Compensation

A covered bank should establish and adhere to processes for talent development, recruitment, and succession planning. The board of directors or appropriate committee should review and approve a written talent management program. A covered bank should also establish and adhere to compensation and performance management programs that comply with any applicable statute or regulation.

Board of Directors Training and Evaluation

The board of directors of a covered bank should establish and adhere to a formal, ongoing training program for all directors. The board of directors should also conduct an annual self-assessment.

Title: OCC Guidelines Establishing Heightened Standards for Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches; Integration of Regulations.

Burden Estimates:

Total Number of Respondents: 31.

Total Burden per Respondent: 3,776.

Total Burden for Collection: 117,056.

Comments are invited on: (1) Whether the proposed collection of information is necessary for the proper performance of the OCC's functions; including whether the information has practical utility; (2) the accuracy of the OCC's estimate of the burden of the proposed information collection, including the cost of compliance; (3) ways to enhance the quality, utility, and clarity of the information to be collected; and (4) ways to minimize the burden of information collection on respondents, including through the use of automated collection techniques or other forms of information technology.

Comments on the collection of information should be sent to:

Because paper mail in the Washington, DC area and at the OCC is subject to delay, commenters are encouraged to submit comments by email if possible. Comments may be sent to: Legislative and Regulatory Activities Division, Office of the Comptroller of the Currency, Attention: 1557–0321, 400 7th Street SW., Suite 3E–218, Mail Stop 9W–11, Washington, DC 20219. In addition, comments may be sent by fax to (571) 465–4326 or by electronic mail to *regs.comments@occ.treas.gov.* You may personally inspect and photocopy comments at the OCC, 400 7th Street SW., Washington, DC 20219. For security reasons, the OCC requires that visitors make an appointment to inspect comments. You may do so by calling (202) 649–6700. Upon arrival, visitors will be required to present valid government-issued photo identification and to submit to security screening in order to inspect and photocopy comments.

All comments received, including attachments and other supporting materials, are part of the public record and subject to public disclosure. Do not enclose any information in your comment or supporting materials that you consider confidential or inappropriate for public disclosure.

You may request additional information on the collection from Johnny Vilela, OCC Clearance Officer, (202) 649–7265, for persons who are deaf or hard of hearing, TTY, (202) 649–5597, Legislative and Regulatory Activities Division, Office of the Comptroller of the Currency, 400 7th

Street SW., Suite 3E–218, Mail Stop 9W–11, Washington, DC 20219.

Additionally, commenters should send a copy of their comments to the OMB desk officer for the agencies by mail to the Office of Information and Regulatory Affairs, U.S. Office of Management and Budget, New Executive Office Building, Room 10235, 725 17th Street NW., Washington, DC 20503; by fax to (202) 395–6974; or by email to *oira.submission@omb.eop.gov.*

Regulatory Flexibility Analysis

The Regulatory Flexibility Act (RFA), 5 U.S.C. 601 *et seq.,* requires generally that, in connection with a rulemaking, an agency prepare and make available for public comment a regulatory flexibility analysis that describes the impact of a rule on small entities. However, the regulatory flexibility analysis otherwise required under the RFA is not required if an agency certifies that the rule will not have a significant economic impact on a substantial number of small entities (defined in regulations promulgated by the Small Business Administration (SBA) to include banking organizations with total assets of less than or equal to $550 million) and publishes its certification and a brief explanatory statement in the **Federal Register** together with the rule.

As of December 31, 2013, the OCC supervised 1,231 small entities based on the SBA's definition of small entities for RFA purposes. As discussed in the **SUPPLEMENTARY INFORMATION** above, the final Guidelines will generally be applicable only to OCC-supervised institutions that have average total consolidated assets of $50 billion or greater; therefore no small entities will be affected by the final Guidelines. Although the application of part 30 to Federal savings associations will affect a substantial number of small Federal savings associations, we do not associate any cost to this change. As such, pursuant to section 605(b) of the RFA, the OCC certifies that these final rules and guidelines will not have a significant economic impact on a substantial number of small entities.

Unfunded Mandates Reform Act Analysis

The OCC has analyzed the final rules and guidelines under the factors in the Unfunded Mandates Reform Act of 1995 (UMRA) (2 U.S.C. 1532). Under this analysis, the OCC considered whether the final rules and guidelines include a Federal mandate that may result in the expenditure by State, local, and tribal governments, in the aggregate, or by the private sector, of $100 million or more in any one year (adjusted annually for inflation). The OCC has determined that the final rules and guidelines will not result in expenditures by State, local, and tribal governments, or the private sector, of $100 million or more in any one year. Accordingly, the final rules and guidelines are not subject to section 202 of the UMRA.

List of Subjects

12 CFR Part 30

Banks, Banking, Consumer protection, National banks, Privacy, Safety and soundness, Reporting and recordkeeping requirements.

12 CFR Part 168

Consumer protection, Privacy, Reporting and recordkeeping requirements, Savings associations, Security measures.

12 CFR Part 170

Accounting, Administrative practice and procedure, Bank deposit insurance, Reporting and recordkeeping requirements, Safety and soundness, Savings associations.

For the reasons set forth in the preamble, and under the authority of 12 U.S.C. 93a, chapter I of title 12 of the Code of Federal Regulations is amended as follows:

PART 30—SAFETY AND SOUNDNESS STANDARDS

1. The authority citation for part 30 is revised to read as follows:

Authority: 12 U.S.C. 1, 93a, 371, 1462a, 1463, 1464, 1467a, 1818, 1828, 1831p-1, 1881–1884, 3102(b) and 5412(b)(2)(B); 15 U.S.C. 1681s, 1681w, 6801, and 6805(b)(1).

§ 30.1 [Amended]

■ 2. Section 30.1 is amended by:
■ a. In paragraph (a):
■ i. Removing ''appendices A, B, and C'' and adding in its place ''appendices A, B, C, and D'';
■ ii. Removing the phrase ''and federal branches of foreign banks,'' and adding in its place the phrase '', Federal savings associations, and Federal branches of foreign banks''; and
■ b. In paragraph (b):
■ i. Removing the word ''federal'' wherever it appears and adding ''Federal'' in its place;
■ ii. Adding the phrase ''Federal savings association, and'' after the phrase ''national bank,'';
■ iii. Removing the phrase ''branch or'' and adding in its place the word ''branch and''; and
■ iv. Adding a comma after the word ''companies''.

■ 3. Section 30.2 is amended by:
■ a. Removing in the second and third sentence the word ''bank'' and adding in its place the phrase ''national bank or Federal savings association''; and
■ b. Adding a final sentence to read as follows:

§ 30.2 Purpose.

* * * The OCC Guidelines Establishing Heightened Standards for Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches are set forth in appendix D to this part.

■ 4. Section 30.3 is amended by:
■ a. Revising the section heading;
■ b. Removing the phrase ''a bank'', wherever it appears, and adding in its place the phrase ''a national bank or Federal savings association'';
■ c. In paragraph (a), removing ''the Interagency Guidelines Establishing Standards for Safeguarding Customer Information set forth in appendix B to this part, or the OCC Guidelines Establishing Standards for Residential Mortgage Lending Practices set forth in appendix C to this part'' and adding in its place ''the Interagency Guidelines Establishing Standards for Safeguarding Customer Information set forth in appendix B to this part, the OCC Guidelines Establishing Standards for Residential Mortgage Lending Practices set forth in appendix C to this part, or the OCC Guidelines Establishing Heightened Standards for Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches set forth in appendix D to this part'';
■ d. In paragraph (b), adding the phrase ''to satisfy'' after the word ''failed''; and
■ e. In paragraph (b), removing the phrase ''the bank'' and adding in its place the phrase ''the bank or savings association''.

The revision reads as follows:

§ 30.3 Determination and notification of failure to meet safety and soundness standards and request for compliance plan.

* * * * *

§ 30.4 [Amended]

■ 5. Section 30.4 is amended by:
■ a. In paragraphs (a), (d), and (e), removing the phrases ''A bank'' and ''a bank'', wherever they appear, and adding in their place the phrases ''A national bank or Federal savings association'' and ''a national bank or Federal savings association'', respectively;
■ b. In paragraph (a), the first sentence of paragraph (d)(1), and in paragraph (e), adding after the phrase ''the bank'', the phrase ''or savings association'';
■ c. In paragraph (b), removing the word ''bank'', and adding in its place the

phrase ''national bank or Federal savings association;

■ d. In paragraph (c), removing the phrase ''bank of whether the plan has been approved or seek additional information from the bank'', and adding in its place the phrase ''national bank or Federal savings association of whether the plan has been approved or seek additional information from the bank or savings association''; and

■ e. In paragraph (d)(1), removing the phrase ''bank commenced operations or experienced a change in control within the previous 24-month period, or the bank'', and adding in its place the phrase ''national bank or Federal savings association commenced operations or experienced a change in control within the previous 24-month period, or the bank or savings association''.

§ 30.5 [Amended]

■ 6. Section 30.5 is amended by:

■ a. Removing the word '' bank'', wherever it appears, except in the first sentence of paragraph (a)(1), and adding in its place the phrase ''national bank or Federal savings association'';

■ b. In paragraph (a)(1), removing the phrase ''bank prior written notice of the OCC's intention to issue an order requiring the bank'', and adding in its place the phrase ''national bank or Federal savings association prior written notice of the OCC's intention to issue an order requiring the bank or savings association''; and

■ c. In the fourth sentence of paragraph (a)(2), removing the word ''matter'' and adding in its place the word ''manner''.

§ 30.6 [Amended]

■ 7. Section 30.6 is amended by:

■ a. Removing the word ''bank'', wherever it appears, and adding in its place the phrase ''national bank or Federal savings association'';

■ b. Adding the phrase '', 12 U.S.C. 1818(i)(1)'' after the word ''Act'' in paragraph (a); and

■ c. Adding the phrase ''12 U.S.C. 1818(i)(2)(A),'' after the word ''Act,'' in paragraph (b).

■ 8. Appendix A to Part 30 is amended by:

■ a. Revising footnote 2; and

■ b. In Section I.B.2. removing the word ''federal'' and adding in its place the word ''Federal''.

The revision reads as follows:

Appendix A to Part 30—Interagency Guidelines Establishing Standards for Safety and Soundness

* * * * *

[2] For the Office of the Comptroller of the Currency, these regulations appear at 12 CFR Part 30; for the Board of Governors of the Federal Reserve System, these regulations appear at 12 CFR part 263; and for the Federal Deposit Insurance Corporation, these regulations appear at 12 CFR part 308, subpart R and 12 CFR part 391, subpart B.

* * * * *

■ 9. Appendix B to part 30 is amended by:

■ a. Removing the words ''bank'' and ''bank's'', wherever they appear, except in Sections I.A. and I.C.2.a., and adding in their place the phrases ''national bank or Federal savings association'' and ''national bank's or Federal savings association's'', respectively; and

■ b. In Section I.A., removing the phrase ''referred to as ''the bank,'' are national banks, federal branches and federal agencies of foreign banks,'' and adding in its place the phrase ''referred to as ''the national bank or Federal savings association,'' are national banks, Federal savings associations, Federal branches and Federal agencies of foreign banks,'';

■ c. In Section I.C.2.d., removing the phrase ''§ 40.3(h) of this chapter'' and adding in its place the phrase ''12 CFR 1016.3(i)'';

■ d. In Section I.C.2.e., removing the phrase ''§ 40.3(n) of this chapter'' and adding in its place the phrase ''12 CFR 1016.3(p)''; and

■ e. In Supplement A to Appendix B to part 30, by revising footnotes 1, 2, 9, 11, and 12.

The revisions read as follows:

Appendix B to Part 30—Interagency Guidelines Establishing Information Security Standards

* * * * *

Supplement A to Appendix B to Part 30—Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice

* * * * *

[1] This Guidance was jointly issued by the Board of Governors of the Federal Reserve System (Board), the Federal Deposit Insurance Corporation (FDIC), the Office of the Comptroller of the Currency (OCC), and the Office of Thrift Supervision (OTS). Pursuant to 12 U.S.C. 5412, the OTS is no longer a party to this Guidance.

[2] 12 CFR part 30, app. B (OCC); 12 CFR part 208, app. D–2 and part 225, app. F (Board); and 12 CFR part 364, app. B and 12 CFR 391.5 (FDIC). The ''Interagency Guidelines Establishing Information Security Standards'' were formerly known as ''The Interagency Guidelines Establishing Standards for Safeguarding Customer Information.''

* * * * *

[9] Under the Guidelines, an institution's *customer information systems* consist of all of the methods used to access, collect, store, use, transmit, protect, or dispose of customer information, including the systems maintained by its service providers. *See* Security Guidelines, I.C.2.d.

* * * * *

[11] *See* Federal Reserve SR Ltr. 13–19, Guidance on Managing Outsourcing Risk, Dec. 5, 2013; OCC Bulletin 2013–29, ''Third-Party Relationships—Risk Management Guidance,'' Oct. 30, 2013; and FDIC FIL 68–99, Risk Assessment Tools and Practices for Information System Security, July 7, 1999.

[12] An institution's obligation to file a SAR is set out in the Agencies' SAR regulations and Agency guidance. *See* 12 CFR 21.11 (national banks, Federal branches and agencies); 12 CFR 163.180 (Federal savings associations); 12 CFR 208.62 (State member banks); 12 CFR 211.5(k) (Edge and agreement corporations); 12 CFR 211.24(f) (uninsured State branches and agencies of foreign banks); 12 CFR 225.4(f) (bank holding companies and their nonbank subsidiaries); 12 CFR part 353 (State non-member banks); and 12 CFR 390.355 (state savings associations). National banks and Federal savings associations must file SARs in connection with computer intrusions and other computer crimes. *See* OCC Bulletin 2000–14, ''Infrastructure Threats—Intrusion Risks'' (May 15, 2000); *see also* Federal Reserve SR 01–11, Identity Theft and Pretext Calling, Apr. 26, 2001.

* * * * *

■ 10. Appendix C to part 30 is amended by:

■ a. In sections I.iv., II.B.1., II.B.2., III.A. introductory text, III.B. introductory text, III.B.6., III.C., III.E.4., and III.E.6., removing the word ''bank'' wherever it appears, and adding in its place the phrase ''national bank or Federal savings association'';

■ b. In section II.B. introductory text and III.D., removing the word ''bank's'' and adding in its place the phrase ''national bank's or Federal savings association's'';

■ c. In sections II.B.1. and III.B.6., removing the word ''bank's'' and adding in its place the phrase ''bank's or savings association's''; and

■ d. Revising the second sentence of section I.i., first two sentences of section I.iii., section I.vi., sections I.A., I.C., I.D.2.b., II.A., III.E. introductory text, III.E.5., and III.F.

The revisions read as follows:

Appendix C to Part 30—OCC Guidelines Establishing Standards for Residential Mortgage Lending Practices

* * * * *

I. * * *

i. * * * The Guidelines are designed to protect against involvement by national banks, Federal savings associations, Federal branches and Federal agencies of foreign banks, and their respective operating subsidiaries (together, ''national banks and Federal savings associations''), either directly or through loans that they purchase or make through intermediaries, in predatory or abusive residential mortgage lending

practices that are injurious to their respective customers and that expose the national bank or Federal savings association to credit, legal, compliance, reputation, and other risks.

* * * * *

* * * * *

iii. In addition, national banks, Federal savings associations, and their respective operating subsidiaries must comply with the requirements and Guidelines affecting appraisals of residential mortgage loans and appraiser independence. 12 CFR part 34, subpart C, and the Interagency Appraisal and Evaluation Guidelines (OCC Bulletin 2010–42 (December 10, 2010). * * *

* * * * *

vi. Finally, OCC regulations and supervisory guidance on fiduciary activities and asset management address the need for national banks and Federal savings associations to perform due diligence and exercise appropriate control with regard to trustee activities. *See* 12 CFR 9.6 (a), in the case of national banks, and 12 CFR 150.200, in the case of Federal savings associations, and the Comptroller's Handbook on Asset Management. For example, national banks and Federal savings associations should exercise appropriate diligence to minimize potential reputation risks when they undertake to act as trustees in mortgage securitizations.

A. *Scope.* These Guidelines apply to the residential mortgage lending activities of national banks, Federal savings associations, Federal branches and Federal agencies of foreign banks, and operating subsidiaries of such entities (except brokers, dealers, persons providing insurance, investment companies, and investment advisers).

* * * * *

C. *Relationship to Other Legal Requirements.* Actions by a national bank or Federal savings association in connection with residential mortgage lending that are inconsistent with these Guidelines or Appendix A to this part 30 may also constitute unsafe or unsound practices for purposes of section 8 of the Federal Deposit Insurance Act, 12 U.S.C. 1818, unfair or deceptive practices for purposes of section 5 of the FTC Act, 15 U.S.C. 45, and the OCC's Lending Rules, 12 CFR 34.3 (Lending Rules) and Real Estate Lending Standards, 12 CFR part 34, subpart D, in the case of national banks, and 12 CFR 160.100 and 160.101, in the case of Federal savings associations, or violations of the ECOA and FHA.

D. * * *

2. * * *

b. *National bank or Federal savings association* means any national bank, Federal savings association, Federal branch or Federal agency of a foreign bank, and any operating subsidiary thereof that is subject to these Guidelines.

II. * * *

A. *General.* A national bank's or Federal savings association's residential mortgage lending activities should reflect standards and practices consistent with and appropriate to the size and complexity of the bank or savings association and the nature and scope of its lending activities.

* * * * *

III. * * *

E. *Purchased and Brokered Loans.* With respect to consumer residential mortgage loans that the national bank or Federal savings association purchases, or makes through a mortgage broker or other intermediary, the national bank or Federal savings association's residential mortgage lending activities should reflect standards and practices consistent with those applied by the bank or savings association in its direct lending activities and include appropriate measures to mitigate risks, such as the following:

* * * * *

5. Loan documentation procedures, management information systems, quality control reviews, and other methods through which the national bank or Federal savings association will verify compliance with agreements, bank or savings association policies, and applicable laws, and otherwise retain appropriate oversight of mortgage origination functions, including loan sourcing, underwriting, and loan closings.

* * * * *

F. *Monitoring and Corrective Action.* A national bank's or Federal savings association's consumer residential mortgage lending activities should include appropriate monitoring of compliance with applicable law and the bank's or savings association's lending standards and practices, periodic monitoring and evaluation of the nature, quantity and resolution of customer complaints, and appropriate evaluation of the effectiveness of the bank's or savings association's standards and practices in accomplishing the objectives set forth in these Guidelines. The bank's or savings association's activities also should include appropriate steps for taking corrective action in response to failures to comply with applicable law and the bank's or savings association's lending standards, and for making adjustments to the bank's or savings association's activities as may be appropriate to enhance their effectiveness or to reflect changes in business practices, market conditions, or the bank's or savings association's lines of business, residential mortgage loan programs, or customer base.

■ 11. A new Appendix D is added to part 30 to read as follows:

Appendix D to Part 30—OCC Guidelines Establishing Heightened Standards for Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches

Table of Contents

I. Introduction
A. Scope
B. Compliance Date
C. Reservation of Authority
D. Preservation of Existing Authority
E. Definitions
II. Standards For Risk Governance Framework
A. Risk Governance Framework
B. Scope of Rrisk Governance Framework
C. Roles and Responsibilities
1. Role and Responsibilities of Front Line Units
2. Role and Responsibilities of Independent Risk Management
3. Role and Responsibilities of Internal Audit
D. Strategic Plan
E. Risk Appetite Statement
F. Concentration and Front Line Unit Risk Limits
G. Risk Appetite Review, Monitoring, and Communication Processes
H. Processes Governing Risk Limit Breaches
I. Concentration Risk Management
J. Risk Data Aggregation and Reporting
K. Relationship of Risk Appetite Statement, Concentration Risk Limits, and Front Line Unit Risk Limits to Other Processes
L. Talent Management Processes
M. Compensation and Performance Management Programs
III. Standards for Board of Directors
A. Require an Effective Risk Governance Framework
B. Provide Active Oversight of Management
C. Exercise Independent Judgment
D. Include Independent Directors
E. Provide Ongoing Training to All Directors
F. Self-Assessments

I. Introduction

1. The OCC expects a covered bank, as that term is defined in paragraph I.E. to establish and implement a risk governance framework to manage and control the covered bank's risk-taking activities.

2. This appendix establishes minimum standards for the design and implementation of a covered bank's risk governance framework and minimum standards for the covered bank's board of directors in providing oversight to the framework's design and implementation (Guidelines). These standards are in addition to any other applicable requirements in law or regulation.

3. A covered bank may use its parent company's risk governance framework in its entirety, without modification, if the framework meets these minimum standards, the risk profiles of the parent company and the covered bank are substantially the same as set forth in paragraph I.4. of these Guidelines, and the covered bank has demonstrated through a documented assessment that its risk profile and its parent company's risk profile are substantially the same. The assessment should be conducted at least annually, in conjunction with the review and update of the risk governance framework performed by independent risk management, as set forth in paragraph II.A. of these Guidelines.

4. A parent company's and covered bank's risk profiles are substantially the same if, as reported on the covered bank's Federal Financial Institutions Examination Council Consolidated Reports of Condition and Income (Call Reports) for the four most recent consecutive quarters, the covered bank's average total consolidated assets, as

calculated according to paragraph I.A. of these Guidelines, represent 95 percent or more of the parent company's average total consolidated assets.[1] A covered bank that does not satisfy this test may submit a written analysis to the OCC for consideration and approval that demonstrates that the risk profile of the parent company and the covered bank are substantially the same based upon other factors not specified in this paragraph.

5. Subject to paragraph I.6. of these Guidelines, a covered bank should establish its own risk governance framework when the parent company's and covered bank's risk profiles are not substantially the same. The covered bank's framework should ensure that the covered bank's risk profile is easily distinguished and separate from that of its parent for risk management and supervisory reporting purposes and that the safety and soundness of the covered bank is not jeopardized by decisions made by the parent company's board of directors and management.

6. When the parent company's and covered bank's risk profiles are not substantially the same, a covered bank may, in consultation with the OCC, incorporate or rely on components of its parent company's risk governance framework when developing its own risk governance framework to the extent those components are consistent with the objectives of these Guidelines.

A. Scope

These Guidelines apply to any bank, as that term is defined in paragraph I.E. of these Guidelines, with average total consolidated assets equal to or greater than $50 billion. In addition, these Guidelines apply to any bank with average total consolidated assets less than $50 billion if that institution's parent company controls at least one covered bank. For a covered bank, average total consolidated assets means the average of the covered bank's total consolidated assets, as reported on the covered bank's Call Reports, for the four most recent consecutive quarters.

B. Compliance Date

1. *Initial compliance.* The date on which a covered bank should comply with the Guidelines is set forth below:

(a) A covered bank with average total consolidated assets, as calculated according to paragraph I.A. of these Guidelines, equal to or greater than $750 billion as of November 10, 2014 should comply with these Guidelines on November 10, 2014;

(b) A covered bank with average total consolidated assets, as calculated according to paragraph I.A. of these Guidelines, equal to or greater than $100 billion but less than $750 billion as of November 10, 2014 should comply with these Guidelines within six months from November 10, 2014;

(c) A covered bank with average total consolidated assets, as calculated according to paragraph I.A. of these Guidelines, equal to or greater than $50 billion but less than $100 billion as of November 10, 2014 should comply with these Guidelines within 18 months from November 10, 2014;

(d) A covered bank with average total consolidated assets, as calculated according to paragraph I.A. of these Guidelines, less than $50 billion that is a covered bank because that bank's parent company controls at least one other covered bank as of November 10, 2014 should comply with these Guidelines on the date that such other covered bank should comply; and

(e) A covered bank that does not come within the scope of these Guidelines on November 10, 2014, but subsequently becomes subject to the Guidelines because average total consolidated assets, as calculated according to paragraph I.A. of these Guidelines, are equal to or greater than $50 billion after November 10, 2014, should comply with these Guidelines within 18 months from the as-of date of the most recent Call Report used in the calculation of the average.

C. Reservation of Authority

1. The OCC reserves the authority to apply these Guidelines, in whole or in part, to a bank that has average total consolidated assets less than $50 billion, if the OCC determines such bank's operations are highly complex or otherwise present a heightened risk as to warrant the application of these Guidelines;

2. The OCC reserves the authority, for each covered bank, to extend the time for compliance with these Guidelines or modify these Guidelines; or

3. The OCC reserves the authority to determine that compliance with these Guidelines should no longer be required for a covered bank. The OCC would generally make the determination under this paragraph I.C.3. if a covered bank's operations are no longer highly complex or no longer present a heightened risk. In determining whether a covered bank's operations are highly complex or present a heightened risk, the OCC will consider the following factors: Complexity of products and services, risk profile, and scope of operations.

4. When exercising the authority in this paragraph I.C., the OCC will apply notice and response procedures, when appropriate, in the same manner and to the same extent as the notice and response procedures in 12 CFR 3.404.

D. Preservation of Existing Authority

Neither section 39 of the Federal Deposit Insurance Act (12 U.S.C. 1831p–1) nor these Guidelines in any way limits the authority of the OCC to address unsafe or unsound practices or conditions or other violations of law. The OCC may take action under section 39 and these Guidelines independently of, in conjunction with, or in addition to any other enforcement action available to the OCC.

E. Definitions

1. *Bank* means any insured national bank, insured Federal savings association, or insured Federal branch of a foreign bank.

2. *Chief Audit Executive* means an individual who leads internal audit and is one level below the Chief Executive Officer in a covered bank's organizational structure.

3. *Chief Risk Executive* means an individual who leads an independent risk management unit and is one level below the Chief Executive Officer in a covered bank's organizational structure. A covered bank may have more than one Chief Risk Executive.

4. *Control.* A parent company *controls* a covered bank if it:

(a) Owns, controls, or holds with power to vote 25 percent or more of a class of voting securities of the covered bank; or

(b) Consolidates the covered bank for financial reporting purposes.

5. *Covered bank* means any bank:

(a) With average total consolidated assets, as calculated according to paragraph I.A. of these Guidelines, equal to or greater than $50 billion;

(b) With average total consolidated assets less than $50 billion if that bank's parent company controls at least one covered bank; or

(c) With average total consolidated assets less than $50 billion, if the OCC determines such bank's operations are highly complex or otherwise present a heightened risk as to warrant the application of these Guidelines pursuant to paragraph I.C. of these Guidelines.

6. *Front Line Unit.* (a) Except as provided in paragraph (b) of this definition, *front line unit* means any organizational unit or function thereof in a covered bank that is accountable for a risk in paragraph II.B. of these Guidelines that:

(i) Engages in activities designed to generate revenue or reduce expenses for the parent company or covered bank;

(ii) 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

(iii) Provides technology services to any organizational unit or function covered by these Guidelines.

(b) *Front line unit* does not ordinarily include an organizational unit or function thereof within a covered bank that provides legal services to the covered bank.

7. *Independent risk management* means any organizational unit within a covered bank that has responsibility for identifying, measuring, monitoring, or controlling aggregate risks. Such units maintain independence from front line units through the following reporting structure:

(a) The board of directors or the board's risk committee reviews and approves the risk governance framework;

(b) Each Chief Risk Executive has unrestricted access to the board of directors and its committees to address risks and issues identified through independent risk management's activities;

(c) The board of directors or its risk committee approves all decisions regarding the appointment or removal of the Chief Risk Executive(s) and approves the annual compensation and salary adjustment of the Chief Risk Executive(s); and

(d) No front line unit executive oversees any independent risk management unit.

8. *Internal audit* means the organizational unit within a covered bank that is designated

[1] For a parent company, average total consolidated assets means the average of the parent company's total consolidated assets, as reported on the parent company's Form FR Y–9C to the Board of Governors of the Federal Reserve System, or equivalent regulatory report, for the four most recent consecutive quarters.

to fulfill the role and responsibilities outlined in 12 CFR part 30, Appendix A, II.B. Internal audit maintains independence from front line units and independent risk management through the following reporting structure:

(a) The Chief Audit Executive has unrestricted access to the board's audit committee to address risks and issues identified through internal audit's activities;

(b) The audit committee reviews and approves internal audit's overall charter and audit plans;

(c) The audit committee approves all decisions regarding the appointment or removal and annual compensation and salary adjustment of the Chief Audit Executive;

(d) The audit committee or the Chief Executive Officer oversees the Chief Audit Executive's administrative activities; and

(e) No front line unit executive oversees internal audit.

9. *Parent company* means the top-tier legal entity in a covered bank's ownership structure.

10. *Risk appetite* means the aggregate level and types of risk the board of directors and management are willing to assume to achieve a covered bank's strategic objectives and business plan, consistent with applicable capital, liquidity, and other regulatory requirements.

11. *Risk profile* means a point-in-time assessment of a covered bank's risks, aggregated within and across each relevant risk category, using methodologies consistent with the risk appetite statement described in paragraph II.E. of these Guidelines.

II. Standards for Risk Governance Framework

A. *Risk governance framework.* A covered bank should establish and adhere to a formal, written risk governance framework that is designed by independent risk management and approved by the board of directors or the board's risk committee. The risk governance framework should include delegations of authority from the board of directors to management committees and executive officers as well as the risk limits established for material activities. Independent risk management should review and update the risk governance framework at least annually, and as often as needed to address improvements in industry risk management practices and changes in the covered bank's risk profile caused by emerging risks, its strategic plans, or other internal and external factors.

B. *Scope of risk governance framework.* The risk governance framework should cover the following risk categories that apply to the covered bank: Credit risk, interest rate risk, liquidity risk, price risk, operational risk, compliance risk, strategic risk, and reputation risk.

C. *Roles and responsibilities.* The risk governance framework should include well-defined risk management roles and responsibilities for front line units, independent risk management, and internal audit.[2] The roles and responsibilities for each of these organizational units should be:

1. *Role and responsibilities of front line units.* Front line units should take responsibility and be held accountable by the Chief Executive Officer and the board of directors for appropriately assessing and effectively managing all of the risks associated with their activities. In fulfilling this responsibility, each front line unit should, either alone or in conjunction with another organizational unit that has the purpose of assisting a front line unit:

(a) Assess, on an ongoing basis, the material risks associated with its activities and use such risk assessments as the basis for fulfilling its responsibilities under paragraphs II.C.1.(b) and (c) of these Guidelines and for determining if actions need to be taken to strengthen risk management or reduce risk given changes in the unit's risk profile or other conditions;

(b) Establish and adhere to a set of written policies that include front line unit risk limits as discussed in paragraph II.F. of these Guidelines. Such policies should ensure risks associated with the front line unit's activities are effectively identified, measured, monitored, and controlled, consistent with the covered bank's risk appetite statement, concentration risk limits, and all policies established within the risk governance framework under paragraphs II.C.2.(c) and II.G. through K. of these Guidelines;

(c) Establish and adhere to procedures and processes, as necessary, to maintain compliance with the policies described in paragraph II.C.1.(b) of these Guidelines;

(d) Adhere to all applicable policies, procedures, and processes established by independent risk management;

(e) Develop, attract, and retain talent and maintain staffing levels required to carry out the unit's role and responsibilities effectively, as set forth in paragraphs II.C.1.(a) through (d) of these Guidelines;

(f) Establish and adhere to talent management processes that comply with paragraph II.L. of these Guidelines; and

(g) Establish and adhere to compensation and performance management programs that comply with paragraph II.M. of these Guidelines.

2. *Role and responsibilities of independent risk management.* Independent risk management should oversee the covered bank's risk-taking activities and assess risks and issues independent of front line units. In fulfilling these responsibilities, independent risk management should:

(a) Take primary responsibility and be held accountable by the Chief Executive Officer and the board of directors for designing a comprehensive written risk governance framework that meets these Guidelines and is commensurate with the size, complexity, and risk profile of the covered bank;

(b) Identify and assess, on an ongoing basis, the covered bank's material aggregate risks and use such risk assessments as the basis for fulfilling its responsibilities under paragraphs II.C.2.(c) and (d) of these Guidelines and for determining if actions need to be taken to strengthen risk management or reduce risk given changes in the covered bank's risk profile or other conditions;

(c) Establish and adhere to enterprise policies that include concentration risk limits. Such policies should state how aggregate risks within the covered bank are effectively identified, measured, monitored, and controlled, consistent with the covered bank's risk appetite statement and all policies and processes established within the risk governance framework under paragraphs II.G. through K. of these Guidelines;

(d) Establish and adhere to procedures and processes, as necessary, to ensure compliance with the policies described in paragraph II.C.2.(c) of these Guidelines;

(e) Identify and communicate to the Chief Executive Officer and the board of directors or the board's risk committee:

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

(ii) Significant instances where a front line unit is not adhering to the risk governance framework, including instances when front line units do not meet the standards set forth in paragraph II.C.1. of these Guidelines;

(f) Identify and communicate to the board of directors or the board's risk committee:

(i) Material risks and significant instances where independent risk management's assessment of risk differs from the Chief Executive Officer; and

(ii) Significant instances where the Chief Executive Officer is not adhering to, or holding front line units accountable for adhering to, the risk governance framework;

(g) Develop, attract, and retain talent and maintain staffing levels required to carry out its role and responsibilities effectively, as set forth in paragraphs II.C.2.(a) through (f) of these Guidelines;

(h) Establish and adhere to talent management processes that comply with paragraph II.L. of these Guidelines; and

(i) Establish and adhere to compensation and performance management programs that comply with paragraph II.M. of these Guidelines.

3. *Role and responsibilities of internal audit.* In addition to meeting the standards set forth in appendix A of part 30, internal audit should ensure that the covered bank's risk governance framework complies with these Guidelines and is appropriate for the size, complexity, and risk profile of the covered bank. In carrying out its responsibilities, internal audit should:

(a) Maintain a complete and current inventory of all of the covered bank's material processes, product lines, services, and functions, and assess the risks, including emerging risks, associated with each, which collectively provide a basis for the audit plan

[2] These roles and responsibilities are in addition to any roles and responsibilities set forth in Appendices A, B, and C to Part 30. Many of the risk management practices established and maintained by a covered bank 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. In addition, existing OCC guidance sets forth standards for establishing risk management programs for certain risks, *e.g.,* compliance risk management. These risk-specific programs should also be considered components of the risk governance framework, within the context of the three units described in paragraph II.C. of these Guidelines.

described in paragraph II.C.3.(b) of these Guidelines;

(b) Establish and adhere to an audit plan that is periodically reviewed and updated that takes into account the covered bank's risk profile, emerging risks, and issues, and establishes the frequency with which activities should be audited. The audit plan should require 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 risk governance framework. Significant changes to the audit plan should be communicated to the board's audit committee;

(c) Report in writing, conclusions and material issues and recommendations from audit work carried out under the audit plan described in paragraph II.C.3.(b) of these Guidelines to the board's audit committee. Internal audit's reports to the audit committee should also identify the root cause of any material issues and include:

(i) 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 bank; and

(ii) A determination of the effectiveness of front line units and independent risk management in identifying and resolving issues in a timely manner;

(d) Establish and adhere to processes for independently assessing the design and ongoing effectiveness of the risk governance framework on at least an annual basis. The independent assessment should include a conclusion on the covered bank's compliance with the standards set forth in these Guidelines; [3]

(e) Identify and communicate to the board's audit committee significant instances where front line units or independent risk management are not adhering to the risk governance framework;

(f) Establish a quality assurance program 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 bank, are updated to reflect changes to internal and external risk factors, emerging risks, and improvements in industry internal audit practices, and are consistently followed;

(g) Develop, attract, and retain talent and maintain staffing levels required to effectively carry out its role and responsibilities, as set forth in paragraphs II.C.3.(a) through (f) of these Guidelines;

(h) Establish and adhere to talent management processes that comply with paragraph II.L. of these Guidelines; and

(i) Establish and adhere to compensation and performance management programs that comply with paragraph II.M. of these Guidelines.

D. *Strategic plan.* The Chief Executive Officer should be responsible for the development of a written strategic plan with input from front line units, independent risk management, and internal audit. The board of directors should evaluate and approve the strategic plan and monitor management's efforts to implement the strategic plan at least annually. The strategic plan should cover, at a minimum, a three-year period and:

1. Contain a comprehensive assessment of risks that currently have an impact on the covered bank or that could have an impact on the covered bank during the period covered by the strategic plan;

2. Articulate an overall mission statement and strategic objectives for the covered bank, and include an explanation of how the covered bank will achieve those objectives;

3. Include an explanation of how the covered bank will update, as necessary, the risk governance framework to account for changes in the covered bank's risk profile projected under the strategic plan; and

4. Be reviewed, updated, and approved, as necessary, due to changes in the covered bank's risk profile or operating environment that were not contemplated when the strategic plan was developed.

E. *Risk appetite statement.* A covered bank should have a comprehensive written statement that articulates the covered bank's risk appetite and serves as the basis for the risk governance framework. The risk appetite statement should include both qualitative components and quantitative limits. The qualitative components should describe a safe and sound risk culture and how the covered bank will assess and accept risks, including those that are difficult to quantify. Quantitative limits should incorporate sound stress testing processes, as appropriate, and address the covered bank's earnings, capital, and liquidity. The covered bank should set limits at levels that take into account appropriate capital and liquidity buffers and prompt management and the board of directors to reduce risk before the covered bank's risk profile jeopardizes the adequacy of its earnings, liquidity, and capital.[4]

F. *Concentration and front line unit risk limits.* The risk governance framework should include concentration risk limits and, as applicable, front line unit risk limits, for the relevant risks. Concentration and front line unit risk limits should limit excessive risk taking and, when aggregated across such units, provide that these risks do not exceed the limits established in the covered bank's risk appetite statement.

G. *Risk appetite review, monitoring, and communication processes.* The risk governance framework should require: [5]

1. Review and approval of the risk appetite statement by the board of directors or the board's risk committee at least annually or more frequently, as necessary, based on the size and volatility of risks and any material changes in the covered bank's business model, strategy, risk profile, or market conditions;

2. Initial communication and ongoing reinforcement of the covered bank's risk appetite statement throughout the covered bank in a manner that causes all employees to align their risk-taking decisions with applicable aspects of the risk appetite statement;

3. Monitoring by independent risk management of the covered bank's risk profile relative to its risk appetite and compliance with concentration risk limits and reporting on such monitoring to the board of directors or the board's risk committee at least quarterly;

4. Monitoring by front line units of compliance with their respective risk limits and reporting to independent risk management at least quarterly; and

5. When necessary due to the level and type of risk, monitoring by independent risk management of front line units' compliance with front line unit risk limits, ongoing communication with front line units regarding adherence to these limits, and reporting of any concerns to the Chief Executive Officer and the board of directors or the board's risk committee, as set forth in paragraphs II.C.2.(e) and (f) of these Guidelines, all at least quarterly.

H. *Processes governing risk limit breaches.* A covered bank should establish and adhere to processes that require front line units and independent risk management, in conjunction 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 bank;

3. Establish protocols for when and how to inform the board of directors, front line unit management, independent risk management, internal audit, and the OCC of a risk limit breach that takes into account the severity of the breach and its impact on the covered bank;

4. Include in the protocols established in paragraph II.H.3. of these Guidelines the requirement to provide a written description of how a breach will be, or has been, resolved; and

5. 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.

I. *Concentration risk management.* The risk governance framework should include policies and supporting processes appropriate for the covered bank's size, complexity, and risk profile for effectively identifying, measuring, monitoring, and controlling the covered bank's concentrations of risk.

J. *Risk data aggregation and reporting.* The risk governance framework should include a set of policies, supported by appropriate procedures and processes, designed to provide risk data aggregation and reporting

[3] The annual independent assessment of the risk governance framework may be conducted by internal audit, an external party, or internal audit in conjunction with an external party.

[4] Where possible, covered banks should establish aggregate risk appetite limits that can be disaggregated and applied at the front line unit level. However, where this is not possible, covered banks should establish limits that reasonably reflect the aggregate level of risk that the board of directors and executive management are willing to accept.

[5] With regard to paragraphs 3., 4., and 5. in this paragraph II.G., the frequency of monitoring and reporting should be performed more often, as necessary, based on the size and volatility of risks and any material change in the covered bank's business model, strategy, risk profile, or market conditions.

capabilities appropriate for the size, complexity, and risk profile of the covered bank, and to support supervisory reporting requirements. Collectively, these policies, procedures, and processes should provide for:

1. The design, implementation, and maintenance of a data architecture and information technology infrastructure that support the covered bank's risk aggregation and reporting needs during normal times and during times of stress;

2. The capturing and aggregating of risk data and reporting of material risks, concentrations, and emerging risks in a timely manner to the board of directors and the OCC; and

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

K. *Relationship of risk appetite statement, concentration risk limits, and front line unit risk limits to other processes.* A covered bank's front line units and independent risk management should incorporate at a minimum the risk appetite statement, concentration risk limits, and front line unit risk limits into the following:

1. Strategic and annual operating plans;

2. Capital stress testing and planning processes;

3. Liquidity stress testing and planning processes;

4. Product and service risk management processes, including those for approving new and modified products and services;

5. Decisions regarding acquisitions and divestitures; and

6. Compensation and performance management programs.

L. *Talent management processes.* A covered bank should establish and adhere to processes for talent development, recruitment, and succession planning to ensure that management and employees who are responsible for or influence material risk decisions have the knowledge, skills, and abilities to effectively identify, measure, monitor, and control relevant risks. The board of directors or an appropriate committee of the board should:

1. Appoint a Chief Executive Officer and appoint or approve the appointment of a Chief Audit Executive and one or more Chief Risk Executives with the skills and abilities to carry out their roles and responsibilities within the risk governance framework;

2. Review and approve a written talent management program that provides for development, recruitment, and succession planning regarding the individuals described in paragraph II.L.1. of these Guidelines, their direct reports, and other potential successors; and

3. Require management to assign individuals specific responsibilities within the talent management program, and hold those individuals accountable for the program's effectiveness.

M. *Compensation and performance management programs.* A covered bank should establish and adhere to compensation and performance management programs that comply with any applicable statute or regulation and are appropriate to:

1. Ensure the Chief Executive Officer, front line units, independent risk management, and internal audit implement and adhere to an effective risk governance framework;

2. Ensure front line unit compensation plans and decisions appropriately consider the level and severity of issues and concerns identified by independent risk management and internal audit, as well as the timeliness of corrective action to resolve such issues and concerns;

3. Attract and retain the talent needed to design, implement, and maintain an effective risk governance framework; and

4. Prohibit any incentive-based payment arrangement, or any feature of any such arrangement, that encourages inappropriate risks by providing excessive compensation or that could lead to material financial loss.

III. Standards for Board of Directors

A. *Require an effective risk governance framework.* Each member of a covered bank's board of directors should oversee the covered bank's compliance with safe and sound banking practices. The board of directors should also require management to establish and implement an effective risk governance framework that meets the minimum standards described in these Guidelines. The board of directors or the board's risk committee should approve any significant changes to the risk governance framework and monitor compliance with such framework.

B. *Provide active oversight of management.* A covered bank's board of directors should actively oversee the covered bank's risk-taking activities and hold management accountable for adhering to the risk governance framework. In providing active oversight, the board of directors may rely on risk assessments and reports prepared by independent risk management and internal audit to support the board's ability to question, challenge, and when necessary, oppose recommendations and decisions made by management that could cause the covered bank's risk profile to exceed its risk appetite or jeopardize the safety and soundness of the covered bank.

C. *Exercise independent judgment.* When providing active oversight under paragraph III.B. of these Guidelines, each member of the board of directors should exercise sound, independent judgment.

D. *Include independent directors.* To promote effective, independent oversight of the covered bank's management, at least two members of the board of directors: [6]

1. Should not be an officer or employee of the parent company or covered bank and has not been an officer or employee of the parent company or covered bank during the previous three years;

2. Should not be a member of the immediate family, as defined in § 225.41(b)(3) of the Board of Governors of the Federal Reserve System's Regulation Y (12 CFR 225.41(b)(3)), of a person who is, or has been within the last three years, an executive officer of the parent company or covered bank, as defined in § 215.2(e)(1) of Regulation O (12 CFR 215.2(e)(1)); and

3. Should qualify as an independent director under the listing standards of a national securities exchange, as demonstrated to the satisfaction of the OCC.

E. *Provide ongoing training to all directors.* The board of directors should establish and adhere to a formal, ongoing training program for all directors. This program should consider the directors' knowledge and experience and the covered bank's risk profile. The program should include, as appropriate, training on:

1. Complex products, services, lines of business, and risks that have a significant impact on the covered bank;

2. Laws, regulations, and supervisory requirements applicable to the covered bank; and

3. Other topics identified by the board of directors.

F. *Self-assessments.* A covered bank's board of directors should conduct an annual self-assessment that includes an evaluation of its effectiveness in meeting the standards in section III of these Guidelines.

PART 168—SECURITY PROCEDURES

■ 12. The authority citation for part 168 continues to read as follows:

Authority: 12 U.S.C. 1462a, 1463, 1464, 1467a, 1828, 1831p–1, 1881–1884, 5412(b)(2)(B); 15 U.S.C. 1681s, 1681w, 6801, and 6805(b)(1).

§ 168.5 [Amended]

■ 13. Section 168.5 is amended by removing the phrase ''part 170'' wherever it appears and adding in its place the phrase ''part 30''.

PART 170 [REMOVED]

■ 14. Remove Part 170.

Dated: September 2, 2014.

Thomas J. Curry,

Comptroller of the Currency.

[FR Doc. 2014–21224 Filed 9–10–14; 8:45 am]

BILLING CODE 4810–33–P

[6] This provision does not supersede other regulatory requirements regarding the composition of the Board that apply to Federal savings associations. These institutions must continue to comply with such other requirements.