DEPARTMENT OF THE TREASURY

Office of the Comptroller of the Currency

12 CFR Parts 30 and 170

[Docket ID OCC-2014-0001]

RIN 1557-AD78

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

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

ACTION: Proposed rules and guidelines.

SUMMARY: The Office of the Comptroller of the Currency (OCC) is requesting comment on proposed guidelines, to be issued as Appendix D to part 30 of its regulations, establishing minimum standards for the design and implementation of a risk governance framework for large insured national banks, insured Federal savings associations, and insured Federal branches of foreign 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 (Guidelines). The standards contained in the Guidelines would 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 also requesting comment on its proposal to make part 30 and its respective appendices applicable to both national banks and Federal savings associations and to remove part 170 as unnecessary. Other technical changes to part 30 are also proposed.

DATES: Comments must be submitted by [INSERT DATE THAT IS 60 DAYS FROM THE DATE OF PUBLICATION]

ADDRESSES: Because paper mail in the Washington, DC area and at the OCC is subject to delay, commenters are encouraged to submit comments through the Federal eRulemaking Portal or e-mail, if possible. Please use the title "OCC Guidelines Establishing Heightened Standards for Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches; Integration of 12 CFR Parts 30 and 170" to facilitate the organization and distribution of the comments. You may submit comments by any of the following methods:

- **Federal eRulemaking Portal—"regulations.gov":** Go to http://www.regulations.gov. Enter "Docket ID OCC-2014-0001" in the Search Box and click "Search". Results can be filtered using the filtering tools on the left side of the screen. Click on "Comment Now" to submit public comments.
- Click on the "Help" tab on the Regulations.gov home page to get information on using Regulations.gov, including instructions for submitting public comments.
- **E-mail:** regs.comments@occ.treas.gov.
- **Mail:** 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.
- **Hand Delivery/Courier:** 400 7th Street, SW., Suite 3E-218, Mail Stop 9W-11, Washington, DC 20219.
- **Fax:** (571) 465-4326.

Instructions: You must include "OCC" as the agency name and "Docket ID OCC-2014-0001" in your comment. In general, the OCC will enter all comments received into the docket and publish them on the Regulations.gov Web site without change, including any business or personal information that you provide such as name and address information, e-mail addresses, or phone numbers. 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 review comments and other related materials that pertain to this rulemaking action by any of the following methods:

- **Viewing Comments Electronically:** Go to http://www.regulations.gov. Enter "Docket ID OCC-2014-0001" in the Search box and click "Search". Comments can be filtered by Agency using the filtering tools on the left side of the screen.
- Click on the "Help" tab on the Regulations.gov home page to get information on using Regulations.gov, including instructions for viewing public comments, viewing other supporting and related materials, and viewing the docket after the close of the comment period.
- **Viewing Comments Personally:** You may personally inspect and photocopy comments at the OCC, 400 7th Street, SW., Washington, DC. 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.

- **Docket:** You may also view or request available background documents and project summaries using the methods described above.

FOR FURTHER INFORMATION CONTACT: For questions concerning the Guidelines, contact Molly Scherf, National Bank Examiner, Large Bank Supervision, (202) 649-7298, or Stuart Feldstein, Director or Andra Shuster, Senior Counsel, Legislative & Regulatory Activities Division, (202) 649-5490, 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. Many governments and central banks across the world, including the U.S. government, responded to the crisis by providing unprecedented levels of support to companies in the financial sector to mitigate the impact of the crisis and to sustain the global financial 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 changes underscore 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.

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

Following 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. The first expectation, often referred to as preserving the sanctity of the charter, maintains that one of the primary fiduciary duties of an institution's board of directors is to ensure that the institution operates in a safe and sound manner. Since large banks are often one of several legal entities under a complex parent company, each bank's board must ensure that the bank does not function simply as a booking entity for its parent and that parent company decisions do not jeopardize the safety and soundness of the bank. This often requires separate and focused governance and risk management practices.

The second expectation generally requires large institutions to have a well-defined personnel management program that ensures appropriate staffing levels, provides for orderly succession, and provides for compensation tools to appropriately motivate and retain talent that does not encourage imprudent risk taking.

The third expectation pertains to risk appetite (or tolerance) and involves institutions defining and communicating an acceptable risk appetite across the organization, including measures that address the amount of capital, earnings, or liquidity that may be at risk on a firm-wide basis, the amount of risk that may be taken in each line of business, and the amount of risk that may be taken in each key risk category monitored by the institution.

The OCC also expects institutions to have reliable oversight programs under the fourth expectation, including the development and maintenance of strong audit and risk management functions. This expectation involves institutions comparing the performance of their audit and

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

risk management functions to the OCC's standards and leading industry practices and taking appropriate action to address material gaps.

The fifth expectation focuses on the board of directors' willingness to provide a credible challenge to bank management's decision-making and thus requests independent directors to acquire a thorough understanding of an institution's risk profile and to use this information to ask probing questions of management and to ensure that senior management prudently addresses risks.

In 2010, the OCC began communicating these heightened expectations informally to institutions in the Large Bank program[3] through our supervisory function. Examiners met with independent directors and executive management from these institutions to discuss the standards and explain how each national bank should apply them.[4] Through its work with the Financial Stability Board (FSB) and Basel Committee on Banking Supervision (BCBS), the OCC found that many supervisors are establishing, or are considering establishing, similar expectations for the financial institutions they regulate. The OCC continued to refine and reinforce the heightened expectations during 2011, and in 2012, started examining each large institution for compliance with the expectations, including documenting its conclusions in the OCC's Report of Examination[5] to reflect each institution's progress in complying with the expectations. Currently, OCC examiners meet with each large institution's management team on a quarterly basis to discuss the institution's progress towards meeting the OCC's heightened expectations.

[3] Entities are included in the OCC's Large Bank program based on asset size and consideration of factors that affect the institution's risk profile and complexity. See Comptroller's Handbook for Bank Supervision Process at 3 (Sept. 2007).

[4] The OCC began applying the heightened expectations standards to Federal savings associations in the Large Bank program in late 2011 after assuming supervisory responsibility for these institutions from the OTS pursuant to the Dodd-Frank Act.

[5] A Report of Examination conveys the overall condition and risk profile of a national bank or Federal savings association, and summarizes examination activities and findings during a supervisory cycle. See Comptroller's Handbook for Bank Supervision Process at 34 (Sept. 2007).

The OCC has also applied aspects of the heightened expectations to institutions in the Midsize Bank program[6] to promote stronger governance and risk management.

Achievement and maintenance of the heightened expectations should help lessen the impact of future economic downturns on large institutions. Therefore, we are proposing standards developed from the heightened expectations in the form of enforceable guidelines. The OCC is proposing to issue the Guidelines as a new Appendix D to part 30 of our regulations. We believe the Guidelines will provide greater certainty to covered institutions and improve examiners' ability to assess compliance with the heightened expectations. As proposed, the Guidelines would be applicable to a broader group of institutions than those currently subject to the heightened expectations program. The proposal generally would apply to insured national banks, insured Federal savings associations, and insured Federal branches of foreign banks with average total consolidated assets of $50 billion or more (together, Banks and each a Bank). The proposal furthers 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. Below, we discuss the enforcement of the Guidelines and provide a detailed description of the standards contained in the Guidelines.

Enforcement of the Guidelines

The OCC is proposing these Guidelines pursuant to section 39 of the Federal Deposit Insurance Act (FDIA).[7] 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

[6] Similar to the Large Bank program, entities are included in the OCC's Midsize Bank program based on asset size and consideration of factors that affect the institution's risk profile and complexity. See Comptroller's Handbook for Bank Supervision Process at 3 (Sept. 2007).

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. For Federal savings associations, these standards are found in Appendices A and B to 12 CFR 170. Part 30, part 170, and Appendices A and B were issued on an interagency basis and are comparable.[8]

Section 39 prescribes different consequences depending on whether the standards it authorizes are issued by regulation or guidelines. Pursuant to section 39, if a national bank or Federal savings association[9] 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 decide whether to require the submission of such a plan.[10] Issuing these heightened standards as guidelines rather than as a regulation provides the OCC with the flexibility to pursue the course of action that is most appropriate given the specific circumstances of a Bank's noncompliance with one or more standards, and the Bank's self-corrective and remedial responses.

---

[7] 12 U.S.C. 1831p-1. Section 39 was enacted as part of the Federal Deposit Insurance Corporation Improvement Act of 1991, P.L. 102-242, section 132(a), 105 Stat. 2236, 2267-70 (Dec. 19, 1991).

[8] As discussed further below, the OCC is also proposing to make part 30 and its appendices applicable to Federal savings associations, and to remove part 170 as it will no longer be necessary.

[9] 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.

[10] 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.

The enforcement remedies prescribed by section 39 are implemented in procedural rules contained in parts 30 and 170 of the OCC's rules. 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 Guidelines.[11] 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 such a 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 is deemed to be in noncompliance with part 30 or part 170, as applicable. Orders are formal, public documents, and

[11] 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 currently are set forth in our regulations at 12 CFR 30.3, 30.4, and 30.5, respectively, for national banks and 12 CFR 170.3, 170.4, and 170.5, respectively, for Federal savings associations.

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 proposed Guidelines consist of three parts. Part I provides an introduction to the Guidelines, explains its scope, and defines key terms used throughout the Guidelines. Part II sets forth the minimum standards for the design and implementation of a Bank's risk governance framework (Framework). Part III provides the minimum standards for the board of directors' (Board) oversight of the Framework.

Part I: Introduction

Under the proposed Guidelines, the OCC would expect a Bank to establish and implement a Framework that manages and controls the Bank's risk taking. The Guidelines establish the minimum standards for the design and implementation of the Framework and the minimum standards for the Board to use in overseeing the Framework's design and implementation. It is important to note 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 Banks to continue to comply with the operational and management standards articulated in Appendix A to part 30, including those related to internal controls, risk management, and management information systems.

If a Bank has a risk profile that is substantially the same as its parent company, the parent company's risk governance framework complies with these Guidelines, and the Bank has demonstrated through a documented assessment that its risk profile and its parent company's risk profile are substantially the same, the Bank may use its parent company's risk governance framework to satisfy the Guidelines. This assessment should be conducted 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 Guidelines. The term "risk profile" is defined in the Guidelines and discussed below. 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% or more of the parent company's average total consolidated assets; (ii) the Bank's total assets under management represent 95% or more of the parent company's total assets under management; and (iii) the Bank's total off-balance sheet exposures represent 95% or more of the parent company's total off-balance sheet exposures. A Bank that does not satisfy this test can 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 Bank would need to develop its own Framework if the parent company's and Bank's risk profiles are not substantially the same. While the Bank may use certain components of the parent company's risk governance framework, 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. This includes ensuring that assets and businesses are not transferred into the 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 Bank. OCC examiners will assist the Bank in determining which components of a parent company's risk governance framework may be used to ensure that the Bank's Framework complies with the Guidelines.

Question 1: The OCC requests comment on the proposed conditions for determining whether a Bank's risk profile is substantially the same as its parent company's risk profile.

Scope. The Guidelines would apply 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 that have average total consolidated assets less than $50 billion as of the effective date of the Guidelines, but subsequently have average total consolidated assets of $50 billion or greater, the date on which the Guidelines would apply to such Banks is the as-of date of the most recent Call Report used in the calculation of the average. Once a Bank becomes subject to the Guidelines because its average total consolidated assets have reached or exceeded the $50 billion threshold, it would be required to continue to comply with the Guidelines even if its average total consolidated assets subsequently drop below $50 billion.

In order to maintain supervisory flexibility, the proposed Guidelines would reserve 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 such entity's operations are highly complex or otherwise present a heightened risk as to require compliance with the Guidelines. In determining whether a 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. For example, these Guidelines will generally apply to a bank with average total consolidated assets less than $50 billion, if the bank's parent company owns more than one bank and the aggregate average total consolidated assets of all of the banks is equal to or greater than

$50 billion. In such cases, the OCC would consider the collective complexity of the banks' products and services, risk profile, and scope of operations.

Conversely, the Guidelines would also reserve the OCC's authority to delay the application of the Guidelines to any Bank, or modify the Guidelines as applicable to certain Banks.[12] Additionally, 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. When exercising any of these reservations of authority, the OCC will apply notice and response procedures, when appropriate, consistent with those set out in 12 CFR 3.404.

The OCC has not included uninsured entities, such as trust banks and Federal branches or agencies of foreign banks, in the scope of the proposed Guidelines because section 39 of the FDIA applies only to "insured depository institutions." Currently, OCC examiners are informally applying certain aspects of the heightened expectations to select uninsured entities. The OCC is considering whether it would be appropriate to apply the provisions in the Guidelines to these entities. The Guidelines could be applied to these entities informally, as is the current practice with the heightened expectations, or the OCC could issue a separate regulation. If the OCC decides to apply the Guidelines informally, we may issue a policy statement to address issues raised by the application of the Guidelines to these institutions. If the Guidelines were to apply to these entities, the OCC would not be able to use the part 30

[12] As previously discussed, the proposed Guidelines would apply to an insured Federal branch of a foreign bank that satisfies the $50 billion average total consolidated asset threshold. Due to the unique nature of insured Federal branches, the OCC has reserved the authority to modify the Guidelines as necessary to tailor the application of the Guidelines to these entities' operations. For example, the OCC expects to tailor the application of Part III of the proposed Guidelines, Standards for Board of Directors, to insured Federal branches because these institutions do not have a Board.

enforcement scheme but would instead need to rely on our enforcement authority with respect to unsafe or unsound practices under 12 U.S.C. 1818.

As discussed above, the Guidelines would be enforceable pursuant to section 39 of the FDIA and part 30 of our rules. Part 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. Paragraph C of Part I includes a number of definitions used throughout the Guidelines. These include: Chief Audit Executive, Chief Risk Executive, front line unit, independent risk management, internal audit, risk appetite, and risk profile. The definitions of risk profile, Chief Audit Executive, and Chief Risk Executive are discussed in the next paragraph and the definitions for the remaining terms will be discussed below under Part II: Standards for Risk Governance Framework.

Risk profile is 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 Guidelines.[13] The term Chief Audit Executive (CAE) means an individual who leads internal audit and is one level below the Chief Executive Officer (CEO) in the Bank's organizational structure.[14] The term Chief Risk Executive (CRE) means an

[13] See proposed Guidelines I.C.7. Independent risk management should prepare this assessment with input from front line units. The Chief Executive Officer, in conjunction with the Board or the Board's risk committee, should ensure that the assessment is comprehensive, understand the assumptions used by independent risk management in preparing the assessment, and recommend changes to the assessment or assumptions that could result in an inaccurate depiction of the bank's risk profile. Internal audit should also provide an independent assessment of the comprehensiveness of the assessment and challenge assumptions that it deems to be inappropriate. As part of their supervisory activities, examiners will assess the integrity of the process used to prepare the assessment and communicate any concerns regarding the process or independent risk management's depiction of the bank's risk profile to the Chief Executive Officer and Board.

[14] See proposed Guidelines I.C.1.

individual who leads an independent risk management unit and is one level below the CEO in the Bank's organizational structure.[15]

Question 2: The OCC requests comment on the advantages and disadvantages of having a single CRE, such as a Chief Risk Officer, provide oversight to all independent risk management units versus having multiple, risk-specific CREs providing oversight to one or more independent risk management units.

Part II: Standards for the Risk Governance Framework

Part II of the proposed Guidelines sets out minimum standards for the design and implementation of a Bank's Framework. Under paragraphs A. and B., a Bank should establish and adhere to a formal, written Framework that covers the following risk categories that apply to the Bank: credit risk, interest rate risk, liquidity risk, price risk, operational risk, compliance risk, strategic risk, and reputation risk. The OCC has defined these eight categories of risks for supervision purposes, but Banks may choose to categorize underlying risks in a different manner for risk management purposes. Regardless of how a Bank categorizes its risks, the Framework must appropriately cover risks to the Bank's earnings, capital, liquidity, and reputation that arise from all of its activities, including risks associated with third-party relationships. Independent risk management should be responsible for the design of the Framework, and for ensuring it comprehensively covers the Bank's risks. Independent risk management should also review and update the Framework at least annually, and as often as needed to address changes in the Bank's risk profile caused by internal or external factors or the evolution of industry risk management

[15] See proposed Guidelines I.C.2. Many Banks designate one CRE, such as a Chief Risk Officer, to oversee all independent risk management units, while other Banks designate risk-specific CREs. In the latter situation, 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 or the Board's risk committee.

practices. The Board or its risk committee would be responsible under this proposal for approving the Framework.

Roles and responsibilities. Paragraph C. sets out the proposed roles and responsibilities for the organizational units that are fundamental to the design and implementation of the Framework. These units are front line units, independent risk management, and internal audit.[16] 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 also ensure that the Board has sufficient information on the Bank's risk profile and risk management practices to provide credible challenges to management's recommendations and decisions. While all three units should ensure that the Board is adequately informed, the independent risk management and internal audit units must have unfettered 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 unfettered access to the Board is critical to ensuring 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. Such expertise can be useful in supplementing internal expertise and providing perspective on industry practices. However, no organizational unit in the Bank may delegate its responsibilities under the Framework to an external party.

[16] The standards set forth in Appendices A and B to part 30 address risk management practices that are fundamental to the safety and soundness of any financial institution, and the standards established in Appendix C to part 30 address risk management practices that are fundamental to the safety and soundness of financial institutions involved in mortgage lending. Many of the risk management practices established and maintained by a Bank to meet these standards should be components of its risk governance framework, within the construct of the three distinct functions identified in the proposed Guidelines. Therefore, Banks subject to Appendix D should ensure that practices established within their Frameworks also meet the standards set forth in Appendices A, B, and C. In addition, existing OCC guidance sets forth standards for establishing risk management programs for certain risks,

1. Role and responsibilities of front line units. The term front line unit means 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,[17] processing,[18] or other support to any organizational unit covered by these Guidelines.[19] The proposed definition of front line units includes those units that provide information technology, operations, servicing, processing, or other support to independent risk management and internal audit. By engaging in these activities, front line units create risks for the Bank.

The Guidelines provide that front line units should own the risks associated with their activities. This means that such units should be responsible for appropriately assessing and effectively managing all risks associated with their activities. Front line units should be held accountable by the CEO and the Board and should meet the standards specified in paragraph II.C.1. Under this paragraph, front line units should assess, on an ongoing basis, the material risks associated with their activities and use these risk assessments as the basis for fulfilling their responsibilities under paragraphs (b) and (c) of paragraph II.C.1. 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) provides that the 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.E. of the proposed Guidelines. These policies should ensure that risks associated with the

---

e.g., compliance risk management. These risk-specific programs should also be considered components of the Framework, within the context of the three functions described in paragraph II.C of the proposed Guidelines.

[17] 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 (if the loan has been sold), maintaining escrow accounts, paying taxes and insurance premiums, and taking steps to collect overdue payments.

[18] Processing refers to activities such as item processing (e.g., sorting of checks), inputting loan, deposit, and other contractual information into information systems, administering collateral tracking systems, etc.

front line units' activities are effectively identified, measured, monitored, and controlled consistent with the Bank's risk appetite statement, concentration risk limits, and certain other of the Bank's policies established within the Framework pursuant to paragraphs II.C.2.(c) and II.G. through K.[20] of the Guidelines. Paragraph (c) provides that front line units should also establish and adhere to procedures and processes necessary to ensure compliance with the aforementioned written policies. For example, 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. The standards articulated in paragraphs (b) and (c) should not be interpreted as an exclusive list of actions front line units should take to effectively manage risk. As discussed above, 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 Bank's risk appetite or applicable concentration risk limits, or the unit's risk limits have not been exceeded. In addition, front line units should adhere to all applicable policies, procedures, and processes established by independent risk management. Front line units should also 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 Guidelines.

2. Roles and responsibilities of independent risk management. The term independent risk management means any organizational unit within the Bank that has responsibility for

[19] See proposed Guidelines I.C.3.

[20] The standards contained in paragraphs II.C.2.(c) and II.G. through K. will be discussed in detail below.

identifying, measuring, monitoring, or controlling aggregate risks.[21] These units maintain independence from front line units by implementing the reporting structure specified in the Guidelines. Specifically, the Board or the Board's risk committee reviews and approves the Framework and any material policies established under the Framework. The Board or its 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 Board or the Board's risk committee receives 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 or the Board's risk committee makes 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 CEO oversees the CRE's day-to-day activities. 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). It also includes, but is not limited to, 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. Finally, no front line unit executive oversees any independent risk management units.

Paragraph II.C.2. of the proposed Guidelines provides 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. In fulfilling these responsibilities, independent risk management should take primary responsibility for designing a Framework commensurate with the Bank's

[21] See proposed Guidelines I.C.2. The OCC understands that various terms are often used to describe this organizational unit (e.g., risk organization, enterprise risk management). For purposes of the Guidelines, the OCC

size, complexity, and risk profile that meets these Guidelines. Independent risk management should also 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) provides that independent risk management should establish and adhere to enterprise policies that include concentration risk limits[22] and that ensure that aggregate risks within the Bank are effectively identified, measured, monitored, and controlled, consistent with the Bank's risk appetite statement and that the Bank's policies and processes established under paragraphs II.G. through K. of the Framework.

Independent risk management also should be held accountable by the CEO and the Board, and paragraphs (d) and (e) provides 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. Independent risk management should also identify and communicate to the CEO and the Board or the Board's risk committee material risks and significant instances where independent risk management's assessment of risk differs from a front line unit as well as significant instances where a front line unit is not complying with the Framework.

The standards articulated in paragraphs (c) and (d) should not be interpreted as an exclusive list of actions independent risk management should take to effectively manage risk. As discussed above, independent risk management should use its risk assessments to determine if

---

proposes to use the term independent risk management.

[22] A concentration of risk refers to an exposure with the potential to produce losses large enough to threaten a bank's financial condition or its ability to maintain its core operations. Risk concentrations can arise in a

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 Bank's risk appetite or applicable concentration risk limits, or a front line unit's risk limits have not been exceeded.

Independent risk management should also identify and communicate to the Board 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 Framework. Finally, 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.

Question 3: Section II.C.3.(a) provides that internal audit should maintain a complete and current inventory of all of the Bank's material businesses, product lines, services, and functions. The OCC requests comment on whether the Guidelines should provide that independent risk management also maintain such an inventory in order to ensure that internal audit has identified all material businesses, product lines, services, and functions.

3. Roles and responsibilities of internal audit. The term internal audit means the organizational unit within the Bank that is designated to fulfill the role and responsibilities outlined in 12 CFR 30 Appendix A, II.B.[23] Internal audit is the third of a Bank's three lines of defense. Paragraph II.C.3. provides that internal audit should ensure that the Bank's Framework complies with the Guidelines and is appropriate for the Bank's size, complexity, and risk profile.

---

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.

Internal audit maintains independence from front line and independent risk management units by implementing the reporting structure specified in the Guidelines. Specifically, the Board's audit committee reviews and approves internal audit's overall charter, risk assessments, and audit plans. In addition, the committee approves all decisions regarding the appointment or removal and annual compensation and salary adjustment of the CAE. The Board's audit committee also receives communications from the CAE on the results of internal audit's activities or other matters that the CAE determines are necessary and makes 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. The CEO oversees the CAE's day-to-day activities. This includes, but is not limited to, budgeting and management accounting, human resource administration, internal communications and information flows, and the administration of the unit's internal policies and procedures. If internal audit reports to the Board's audit committee, the audit committee or its chair would fill the aforementioned role of the CEO. Finally, no front line unit executive oversees internal audit.

The design and implementation of the audit plan is an important element of internal audit's role and responsibilities under the Framework. 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. This inventory and assessment will form the basis of the audit plan. The audit plan should rate the risk presented by each front line unit, product line, service, and function. This includes activities that the Bank may outsource to a third party. Internal audit should derive these 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. The audit plan should include

[23] See proposed Guidelines I.C.5.

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. The audit plan should be updated at least quarterly and should take into account the Bank's risk profile as well as emerging risks and issues. 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. This 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 Bank. All changes to the audit plan should be communicated to the Board's audit committee.

Internal audit should report in writing to the Board's 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. The report also should address potential and emerging concerns, the timeliness of corrective actions, and the status of outstanding issues. These reports should include objective measures that enable the identification, measurement, and monitoring of risk and internal control issues. Finally, audit reports should include comments on the effectiveness of front line units in

identifying excessive risks and issues, emerging issues, and the appropriateness of risk levels relative to both the quality of the internal controls and the risk appetite statement.

Internal audit should also establish and adhere to processes for independently assessing the design and effectiveness of the Framework. The assessment should be done 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. Internal audit should also communicate to the Board's audit committee significant instances where front line units or independent risk management are not adhering to the Framework. Internal audit should also establish a quality assurance department 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 to risk factors, and are consistently followed. Internal audit should also 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 Guidelines.

Question 4: The OCC requests 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. Is such an assessment possible for internal audit given the wide range of practices in the industry and the challenges associated with determining what constitutes a leading industry practice? Are there any other concerns with such a requirement?

4. Stature. For the Framework to be effective, it is critical that independent risk management and internal audit have the stature needed to effectively carry out their respective

roles and responsibilities. This stature is generally evidenced by the attitudes and level of support provided by the Board, CEO, and others within the Bank toward these units. The Board 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 the Board's oversight responsibilities set forth in Part III of the proposed 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 Part II of the proposed Guidelines provides that the CEO should develop a written strategic plan with input from front line units, independent risk management, and internal audit. The Board should evaluate and approve the strategic plan and monitor management's efforts to implement it at least annually. At a minimum, the strategic plan should cover a three-year period and should contain a comprehensive assessment of risks that currently impact the Bank or that could impact 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 strategic plan should also include an explanation of how the Bank will update, as necessary, the Framework to account for changes in the Bank's risk profile projected under the strategic plan. Finally, the strategic plan should be reviewed, updated, and approved, as necessary, due to changes in the Bank's risk profile or operating environment that were not contemplated when the strategic plan was developed.

Risk appetite statement. Paragraph E. of Part II of the proposed Guidelines provides that the Bank should have a comprehensive written statement that articulates the 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.[24] The Board and management should ensure that the level and types of risk they are willing to assume to achieve the Bank's strategic objectives and business plan are consistent with its capital and liquidity needs and requirements, as well as other laws and regulatory requirements applicable to the Bank.

The Statement should include both qualitative components and quantitative limits. The qualitative components of the Statement should describe a safe and sound "risk culture"[25] and how the Bank will assess and accept risks, including those that are difficult to quantify, on a consistent basis throughout the Bank. 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 Bank to share when carrying out their respective roles and responsibilities within the Bank. These values should serve as the basis for risk-taking decisions made throughout the Bank and should be reinforced by the actions of the Board, executive management, Board committees, and individuals. 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

[24] See proposed Guidelines I.C.6.

[25] 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 Bank that shape and influence governance practices and risk decisions.

quantitative limits established in the Statement, and hold accountable those who do not conduct themselves in a manner consistent with these articulated standards.

Quantitative limits should incorporate sound stress testing processes, as appropriate, and should address the Bank's earnings, capital, and liquidity positions. The Bank may set quantitative limits on a gross or net basis that take into account appropriate capital and liquidity buffers; in either case, these limits should be set at levels that prompt management and the Board to manage risk proactively before the Bank's risk profile jeopardizes the adequacy of its earnings, liquidity, and capital. 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. Examiners will apply judgment when determining which quantitative limits should be based on stress testing. They will consider several factors, including the value in using such measures for the risk type, the Bank's ability to produce such measures, the capabilities of similarly-situated institutions, and the degree to which the Bank's Board and management have invested in the resources needed to establish such capabilities. The Federal banking agencies issued guidance on stress testing in May 2012.[26] The guidance describes various stress testing approaches and applications, and 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

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

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

Concentration and front line unit risk limits. Paragraph F. of Part II of the proposed Guidelines provides 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. When aggregated across all such units, the risks should not exceed the limits established in the Bank's Statement. Depending on a Bank's organizational structure, concentration risk limits and front line unit risk limits may also need to be established for legal entities, units based on geographical areas, or product lines.

Risk appetite review, monitoring, and communication processes. Paragraph G. of Part II of the proposed Guidelines provides 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 and independent risk management 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. With regard to the monitoring and reporting set forth in paragraph G., 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 Bank's business model, strategy, risk profile, or market conditions.

Processes governing risk limit breaches. Paragraph H. of Part II of the proposed Guidelines sets out processes governing risk limit breaches. 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 Bank should also 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. It is acceptable for Banks to have different escalation and resolution processes for breaches of the Statement, concentration risk limits, and front line unit risk limits. However, both processes are important elements of the overall Framework.

Concentration risk management. Paragraph I. of Part II of the proposed Guidelines provides 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. 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 exclusive; any product or service may expose a bank to multiple risks and risks may also be interdependent.[27] Furthermore, concentrations can exist on and off the balance sheet. 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.[28]

Risk data aggregation and reporting. Paragraph J. of Part II of the proposed Guidelines addresses risk data aggregation and reporting. This paragraph provides that the Framework should include a set of policies, supported by appropriate procedures and processes, designed to ensure that the Bank's risk data aggregation and reporting capabilities are appropriate for its size, complexity, and risk profile and support supervisory reporting requirements. These policies, procedures, and processes should provide for an information technology (IT) infrastructure that supports the Bank's risk aggregation and reporting needs in both normal times and times of stress. Processes should capture aggregate risk data and report material risks, concentrations, and emerging risks to the Board and the OCC in a timely manner. In addition, these policies,

[27] See Comptroller's Handbook for Large Bank Supervision at 4 (Jan. 2010).

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

procedures, and processes should provide for the distribution of risk reports to all relevant parties at a frequency that meets the recipients' needs for decision-making purposes.

During the financial crisis, it became apparent that many banks' IT and data architectures were inadequate to support the broad management of financial risks. Many banks lacked the ability to aggregate risk exposures and identify concentrations quickly and accurately at the bank level, across business lines, and among legal entities. The OCC expects Banks to have risk aggregation and reporting capabilities that meet the Board's and management's needs for proactively managing risk and ensuring the Bank's risk profile remains consistent with its risk appetite.[29]

Relationship of risk appetite statement, concentration risk limits, and front line unit risk limits to other processes. Paragraph K. of Part II of the proposed Guidelines addresses the relationship between the Statement, concentration risk limits, and front line unit risk limits to other Bank processes. The Bank's front line units and independent risk management should incorporate these elements 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; compensation and performance management programs. Paragraphs L. and M. of Part II of the proposed Guidelines address the Bank's talent

[29] In January 2013, the BCBS issued a set of principles for effective risk data aggregation and reporting and established the expectation that Global Systemically Important Banks (G-SIBs) comply with these principles by the beginning of 2016. The OCC expects the G-SIBs it supervises to be largely compliant with these principles by the date established by the BCBS. Other Banks covered by these Guidelines are not expected to comply with the BCBS principles by the beginning of 2016; however, their risk aggregation and reporting capabilities should be sufficiently robust to meet the Bank's needs. These Banks should consider the BCBS principles to be leading practices and should make an effort to bring their practices into alignment with the principles where possible.

management processes and compensation and performance management programs, respectively. With regard to talent management, the proposal provides that the Bank should establish and adhere to processes for talent development, recruitment, and succession planning to ensure that those 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. A Bank's talent management processes should ensure that the Board or a Board committee: (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. In addition, these processes should ensure that the Board or a Board committee: (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.

With regard to compensation and performance management programs, the Bank should establish and adhere to programs that meet the requirements of any applicable statute or regulation. 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 programs should also 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. The programs should be designed to attract and retain the talent needed to design, implement, and maintain an effective Framework. In addition, 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.[30]

Part III: Standards for Board of Directors

Part III of the proposed Guidelines sets out the minimum standards for the Bank's Board in providing oversight to the Framework's design and implementation.

Ensure an effective risk governance framework. Paragraph A. of Part III of the proposed Guidelines provides that each member of the Board has a duty to oversee the Bank's compliance with safe and sound banking practices. Consistent with this duty, the Board should ensure that the Bank establishes and implements an effective Framework that complies with the Guidelines. The Board or its risk committee should also approve any changes to the Framework.

Provide active oversight of management. Paragraph B. of Part III of the proposed Guidelines addresses Board oversight of Bank management, and generally provides that the Board should provide a credible challenge to management. Specifically, the Board should actively oversee the Bank's risk-taking activities and hold management accountable for adhering to the Framework. The Board should also critically evaluate management's recommendations and decisions by questioning, challenging, and, when necessary, opposing, 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. The OCC expects that this provision will enable the Board to make a determination as to whether management is adhering to, and understands, the

[30] This standard was adapted from the standard set out in section 956 of the Dodd-Frank Act. We note that the OCC, the Board of Governors of the Federal Reserve System (FRB), 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). In addition, section 956 of the Dodd-Frank Act requires the OCC, the FRB, the FDIC, the National Credit Union Administration, the Securities and Exchange Commission, and the Federal Housing Finance Agency (the Agencies) to jointly prescribe incentive-based

Framework. For example, recurring breaches of risk limits or actions that cause the Bank's risk profile to materially exceed its risk appetite may demonstrate that management is not adhering to the Framework. In those situations, the Board should take action to hold the appropriate party, or parties, accountable.

Exercise independent judgment. Paragraph C. of Part III of the proposed Guidelines provides that each Board member should exercise sound, independent judgment. In determining whether a Board member is adequately objective and independent, the OCC will consider the degree to which the Board member's other responsibilities conflict with his or her ability to act in the Bank's best interests.

Include independent directors. Paragraph D. of Part III of the proposed Guidelines provides that at least two members of a Bank's Board should be independent, i.e., they should not be members of the Bank's or the parent company's management. This Guideline would enable the Bank's Board to provide effective, independent oversight of Bank management. To the extent the Bank's independent directors are also members of the parent company's Board, the OCC expects 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 OCC notes that this standard does not supersede other applicable regulatory requirements concerning the composition of a Federal savings association's Board.[31] These associations must continue to comply with such requirements.

Question 5: The OCC requests comment on the composition of a Bank's Board. The proposed Guidelines establish a minimum number of independent directors that should be on the Bank's Board. Is this an appropriate number? Are there other standards the OCC should

---

regulations or guidelines applicable to covered institutions. To date, the Agencies have issued a Notice of Proposed Rulemaking. See 76 FR 21170 (April 14, 2011).

consider to ensure the Board composition is adequate to provide effective oversight of the Bank? Is there value in requiring the Bank to maintain its own risk committee and other committees, as opposed to permitting the Bank's Board to leverage the parent company's Board committees?

Provide ongoing training to independent directors. Paragraph E. of Part III provides that in order to ensure that each member of the Board 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 independent directors. This reflects the OCC's view that the Board should be comprised of financially knowledgeable directors who are committed to conducting diligent reviews of the 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. The training program for independent directors 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.

Self-assessments. Finally, Paragraph F. of Part III of the proposed Guidelines provides that the Bank's Board should conduct an annual self-assessment that includes an evaluation of the Board's effectiveness in meeting the standards provided in Part III of the Guidelines. The self-assessment discussed in this paragraph can be part of a broader self-assessment process conducted by the Board, 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 composition and structure, meeting frequency and agenda items, Board

[31] See 12 CFR 163.33.

report design or content, ongoing training program design or content, and other process and procedure topics.

Description of Technical Amendments to Part 30

We are also proposing technical conforming amendments to the part 30 regulations to add references to new Appendix D, which contains the Guidelines, where appropriate.

The Guidelines would be 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.

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 proposes to make part 30 and its respective appendices applicable to both national banks and Federal savings associations, as described below. The OCC also proposes to remove part 170, as it will no longer be necessary, and to make other minor changes to part 30, including the deletion of references to rescinded OTS guidance.

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.[32] 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.[33]

In order to streamline and consolidate the safety and soundness rules applicable to national banks and Federal savings associations, the OCC proposes to apply part 30 to Federal savings associations. Under this proposal, Federal savings associations would not be subject to

---

[32] See 60 FR 35674.

any new requirements but would be subject to the § 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 would provide greater clarity and guidance to Federal savings associations on when 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, the OCC proposes to amend Appendix A to part 30 so that it also applies to Federal savings associations. This proposal 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

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

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.[34] 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 proposes to amend Appendix B to part 30 so that it also applies to Federal savings associations. This proposal 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.[35] 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.

[34] 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).

[35] 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).

While there is no equivalent to Appendix C in part 170, Federal savings associations are subject to guidance on residential mortgage lending.[36] 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 now proposes to apply Appendix C to Federal savings associations. Under this proposal, 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 will clarify the residential mortgage lending standards applicable to these institutions and enhance 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.

Request for Comments

In addition to the questions presented above, the OCC requests comment on all aspects of these proposed rules and guidelines.

Regulatory Analysis

Paperwork Reduction Act

[36] See Examination Handbook Section 212, "One- to Four- Family Residential Real Estate Lending" (Feb. 10, 2011) (incorporating Regulatory Bulletin 37-18 (Mar. 31, 2007)); see also Examination Handbook Section 212C.1, "Interagency Guidance on High Loan-to-Value Residential Real Estate Lending" (Feb. 10. 2011) (incorporating Thrift Bulletin 72a (Oct. 13, 1999)).

The OCC has determined that this proposed rule involves collections of information 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 is seeking a new control number for this collection from OMB and has submitted this collection to OMB.

Abstract

The collection of information is 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.

Standards for Risk Governance Framework

Front Line Units

Banks are required to establish and adhere to a formal, written risk governance framework that is designed by independent risk management, approved by the Board or the Board's risk committee, and reviewed and updated annually by independent risk management.

Independent Risk Management

Independent risk management should oversee the bank's risk-taking activities and assess risks and issues independent of the CEO and front line units by: (i) designing a comprehensive written Framework commensurate with the size, complexity, and risk profile of the Bank; (ii) identifying and assessing, on an ongoing basis, the 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; (v) ensuring that front line units meet required standards; (vi) identifying and communicating to the CEO and Board 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 Framework; (vii) identifying and communicating to the Board 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 Framework; and (viii) 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 Bank's Framework complies with these Guidelines and is appropriate for the size, complexity, and risk profile of the Bank. It 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, which collectively provide a basis for the audit plan. It should establish and adhere to an audit plan, updated at least quarterly, that takes into account the Bank's risk profile, emerging risks, and issues. 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. Changes to the audit plan should be communicated to the Board's audit committee. Internal audit should report in writing, conclusions, 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 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 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 effectiveness of the Framework on at least an annual basis. The independent assessment should include a conclusion on the Bank's compliance with the standards set forth in these Guidelines and the degree to which the Bank's Framework is consistent with leading industry practices. Internal audit should identify and communicate to the Board or Board's audit committee significant instances where front line units or independent risk management are not adhering to the Framework. Internal audit should establish a quality assurance department 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. Internal audit should develop, attract, and retain talent and maintain staffing levels required to effectively carry out the unit's 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.

Concentration Risk Management

The Framework should include policies and supporting processes appropriate for the Bank's size, complexity, and risk profile for effectively identifying, measuring, monitoring, and controlling the Bank's concentration of risk.

Risk Data Aggregation and Reporting

This Framework should include a set of policies, supported by appropriate procedures and processes, designed to ensure that the Bank's risk data aggregation and reporting capabilities are appropriate for its size, complexity, and risk profile and support supervisory reporting requirements. Collectively, these policies, procedures, and processes should provide for: (i) the design, implementation, and maintenance of a data architecture and information technology infrastructure that supports the 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 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.

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

Burden Estimates:

Total Number of Respondents: 21.

Total Burden per Respondent: 7,200.

Total Burden for Collection: 151,200.

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 e-mail if possible. Comments may be sent to: Legislative and Regulatory Activities Division, Office of the Comptroller of the Currency, Attention: [1557-NEW], 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, 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

Pursuant to section 605(b) of the Regulatory Flexibility Act, 5 U.S.C. 605(b) (RFA), the regulatory flexibility analysis otherwise required under section 603 of the RFA is not required if the agency certifies that the proposed rule will not, if promulgated, have a significant economic impact on a substantial number of small entities (defined for purposes of the RFA to include banks and Federal branches and agencies with assets less than or equal to $500 million and trust companies with assets less than or equal to $35.5 million) and publishes its certification and a short, explanatory statement in the Federal Register along with its proposed rule.

The proposed Guidelines would have no impact on any small national banks or Federal branches and agencies or trust companies, as defined by the RFA. The proposed Guidelines would apply only to insured national banks, insured Federal savings associations, and insured Federal branches of a foreign bank with $50 billion or more in average total consolidated assets. The proposed Guidelines reserve the OCC's authority to apply them to an insured national bank, insured Federal savings association, or insured Federal branch of a foreign bank with less than $50 billion in average total consolidated assets if the OCC determines such entity's operations are highly complex or otherwise present a heightened risk. We do not expect any small entities will be determined to have highly complex operations or present heightened risk by the OCC.

The proposal would apply part 30 and its respective appendices to Federal savings associations. As described in the proposal, the guidelines in Appendices A and B of part 30 are substantively the same for national banks and Federal savings associations. The proposal would

apply Appendix C of part 30 to Federal savings associations for the first time. Appendix C consists of guidelines establishing standards for residential mortgage lending practices. Although Federal savings associations are not currently subject to the standards in Appendix C, they are currently subject to guidance on residential mortgage lending. We believe applying part 30 to Federal savings associations will not subject these institutions to substantively different standards relative to their current requirements. Therefore, we estimate that applying part 30 to Federal savings associations introduces only de minimis costs associated with updating compliance requirements.

Therefore, the OCC certifies that the proposed Guidelines would not, if issued, have a significant economic impact on a substantial number of small entities.

Unfunded Mandates Reform Act Analysis

Section 202 of the Unfunded Mandates Reform Act of 1995 (2 U.S.C. 1532), requires the OCC to prepare a budgetary impact statement before promulgating a rule that includes 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 this proposed rule 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 OCC has not prepared a budgetary impact statement.

12 CFR part 30 List of Subjects

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

12 CFR part 170 List of Subjects

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(a) is amended by:

a. In paragraph (a), by:

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), by:

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”.

§ 30.2 [Amended]

3. Section 30.2 is amended by:

i. Removing in the second and third sentence the word “bank” and adding in its place the phrase “national bank or Federal savings association”.

ii. Adding a final sentence to read as follows “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.”

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

4. Section 30.3 is amended by:

a. Revising the heading to read as set forth above;

b. Removing the word “bank”, wherever it appears, and adding in its place the phrase “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.”; and

d. In paragraph (b), adding the phrase “to satisfy” after the word “failed”.

§ 30.4 [Amended]

5. Section 30.4 is amended by:

a. 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 phrases “the bank”, “The bank”, “a bank”, “A bank”, and “Any bank”, wherever they appear, except in the first sentence of paragraph (a)(1), and adding in their place the phrases “the national bank or Federal savings association”, “The

national bank or Federal savings association", "a national bank or Federal savings association", "A national bank or Federal savings association", and "Any national bank or Federal savings association", respectively; and

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"; and

b. Adding the phrases ", 12 U.S.C. 1818(i)(1)" and ", 12 U.S.C. 1818(i)(2)(A)" after the word "Act" in paragraphs (a) and (b), respectively.

8. Appendix A to Part 30 is amended by:

a. Revising footnote 2 to read as follows; and

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

The revision reads as set forth below.

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.

*** * * * ***

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

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 “as “the bank,” are national banks, federal branches and federal”, and by adding in its place the phrase “as “the national bank or Federal savings association,” are national banks, Federal savings associations, Federal branches and Federal”.

10. Supplement A to Appendix B to part 30 is amended by revising footnotes 1, 2, 9, 11, and 12 to read as follows:

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 (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," Nov. 1, 2001; 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); and 12 CFR part 353 (State non-member banks). 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; SR 97–28, Guidance Concerning Reporting of Computer Related Crimes by Financial Institutions, Nov. 6, 1997; and FDIC FIL 48–2000, Suspicious Activity Reports, July 14, 2000; FIL 47–97, Preparation of Suspicious Activity Reports, May 6, 1997.

*** * * * ***

11. Appendix C to part 30 is amended by:

a. In sections I.iv., II.B.2., III.A. introductory text, III.B. introductory text, III.C., and 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 I.ii., removing the phrase "34.3 (Lending Rules).", and adding in its place the phrase "34, subpart D in the case of national banks, and 12 CFR 160.100 and 160.101, in the case of Federal savings associations (Real Estate Lending Standards).";

c. In section I.vi., adding the phrase "and Federal savings associations" after the word "banks", wherever it appears;

d. 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";

e. In sections II.B.1. and III.B.6., removing the words "bank" and "bank's" and adding in their place the phrases "national bank or Federal savings association" and "bank's or savings association's", respectively; and

f. Revising the second sentence of Section I.i., first two sentences of section I.iii., Sections I.v., I.A., I.C., I.D.2.b., II.A., III.E. introductory text, III.E.5., and III.F. to read as follows.

The revisions read as set forth below.

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, the "national bank and Federal savings association"), 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).

* * *

* * * * *

v. OCC regulations also prohibit national banks and their respective operating subsidiaries from providing lump sum, single premium fees for debt cancellation contracts and debt suspension agreements in connection with residential mortgage loans. 12 CFR 37.3(c)(2). Some lending practices and loan terms, including financing single premium credit insurance and

the use of mandatory arbitration clauses, also may significantly impair the eligibility of a residential mortgage loan for purchase in the secondary market.

* * * * *

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 Real Estate Lending Standards, 12 CFR 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.

12. 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

1. The OCC expects a bank, as defined herein, to establish and implement a risk governance framework for managing and controlling the bank's risk-taking activities.

2. This appendix establishes minimum standards for the design and implementation of a bank's risk governance framework and minimum standards for the bank's board of directors[1] 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 bank may use its parent company's risk governance framework if the framework meets these minimum standards, the risk profiles of the parent company and the bank are substantially the same as set forth in paragraph 4., and the 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 or more often, in conjunction with the review and update of the risk governance framework performed by independent risk management, as set forth in paragraph II.A.

4. 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"):

(i) The bank's average total consolidated assets represent 95% or more of the parent company's average total consolidated assets;

(ii) The bank's total assets under management represent 95% or more of the parent company's total assets under management; and

(iii) The bank's total off-balance sheet exposures represent 95% or more of the parent company's total off-balance sheet exposures.

[1] In the case of an insured Federal branch of a foreign bank, the board of directors means the managing official in charge of the branch.

A bank that does not satisfy this test may 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 upon other factors not specified in this paragraph.

5. In cases where the parent company's and bank's risk profiles are not substantially the same, a bank should establish its own risk governance framework. Such a framework should ensure that the 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 bank is not jeopardized by decisions made by the parent company's board of directors and management.

A. Scope

These Guidelines apply to 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 [EFFECTIVE DATE] of these Guidelines (together "banks" and each, a "bank"). Average total consolidated assets is calculated as the average of the bank's total consolidated assets, as reported on the bank's Call Reports, for the four most recent consecutive quarters. The date on which the Guidelines apply to a bank that does not come within the scope of these Guidelines on [EFFECTIVE DATE], but subsequently becomes subject to the Guidelines because average total consolidated assets are equal to or greater than $50 billion after [EFFECTIVE DATE], shall be the as-of date of the most recent Call Report used in the calculation of the average.

The OCC reserves the authority:

(i) To apply these Guidelines to an insured national bank, insured Federal savings association, or insured Federal branch of a foreign bank that has average total consolidated assets less than $50 billion, if the OCC determines such entity's operations are highly complex or otherwise present a heightened risk as to warrant the application of these Guidelines;

(ii) For each bank, to extend the time for compliance with these Guidelines or modify these Guidelines; or

(iii) To determine that compliance with these Guidelines should no longer be required for each bank.

The OCC would generally make the determination in (iii) if a bank's operations are no longer highly complex or no longer present a heightened risk. When exercising the authority in this paragraph, 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.

In determining whether a 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.

B. 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.

C. Definitions

1. Chief Audit Executive is an individual who leads internal audit and is one level below the Chief Executive Officer in the bank's organizational structure.

2. Chief Risk Executive is an individual who leads an independent risk management unit and is one level below the Chief Executive Officer in the bank's organizational structure.

3. Front line unit is 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 these Guidelines.

4. Independent risk management is any organizational unit within the 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:

(i) The board of directors or the board's risk committee reviews and approves the risk governance framework and any material policies established under it. In addition, the board or its risk committee approves all decisions regarding the appointment or removal of the Chief Risk Executive and approves the annual compensation and salary adjustment of the Chief Risk Executive;

(ii) The Chief Executive Officer oversees the Chief Risk Executive's day-to-day activities; and

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

5. Internal audit is 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. Internal audit maintains independence from front line and independent risk management units through the following reporting structure:

(i) The board's audit committee reviews and approves internal audit's overall charter, risk assessments, and audit plans. In addition, the committee approves all decisions regarding the appointment or removal and annual compensation and salary adjustment of the Chief Audit Executive;

(ii) The Chief Executive Officer oversees the Chief Audit Executive's day-to-day activities;[2] and

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

6. Risk appetite is 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.

7. Risk profile is 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 these Guidelines.

II. STANDARDS FOR RISK GOVERNANCE FRAMEWORK

[2] In some banks, the audit committee may assume the Chief Executive Officer's responsibilities to oversee the Chief Audit Executive's day-to-day activities. This is an acceptable alternative under the Guidelines.

A. Risk governance framework. The 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. Independent risk management should review and update the risk governance framework at least annually, and as often as needed to address changes in the bank's risk profile caused by internal or external factors or the evolution of industry risk management practices.

B. Scope of risk governance framework. The risk governance framework should cover the following risk categories that apply to the 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 three distinct functions: front line units, independent risk management, and internal audit.[3] The roles and responsibilities for each of these functions are:

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:

[3] The standards set forth in appendices A and B address risk management practices that are fundamental to the safety and soundness of any financial institution, and the standards established in appendix C address risk management practices that are fundamental to the safety and soundness of financial institutions involved in mortgage lending. Many of the risk management practices established and maintained by a bank to meet these standards should be components of its risk governance framework, within the construct of the three distinct functions described in this paragraph II.C. Therefore, banks subject to appendix D should ensure that practices established within their risk governance frameworks also meet the standards set forth in appendices A, B, and C. In addition, existing OCC guidance sets expectations for banks to establish 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 functions described in paragraph II.C.

(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 1.(b) and 1.(c) 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. Such policies should ensure risks associated with the front line unit's activities are effectively identified, measured, monitored, and controlled, consistent with the 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.;

(c) Establish and adhere to procedures and processes, as necessary to ensure compliance with the policies described in paragraph 1.(b);

(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 1.(a) through 1.(d);

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

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

2. Role and responsibilities of independent risk management. Independent risk management should oversee the bank's risk-taking activities and assess risks and issues independent of the Chief Executive Officer and 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 bank;

   (b) 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 2.(c) and 2.(d) 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;

   (c) Establish and adhere to enterprise policies that include concentration risk limits. Such policies should 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 within the risk governance framework under paragraphs II.G. through K.;

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

(e) Ensure that front line units meet the standards set forth in paragraph II.C.1.;

(f) 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;

(g) 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;

(h) 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 2.(a) through 2.(g);

(i) Establish and adhere to talent management processes that comply with paragraph II.L.; and

(j) Establish and adhere to compensation and performance management programs that comply with paragraph II.M.

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 bank's risk governance framework complies with these Guidelines and is appropriate for the size, complexity, and risk profile of the bank. In carrying out its responsibilities, internal audit should:

(a) 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, which collectively provide a basis for the audit plan described in paragraph 3.(b);

(b) Establish and adhere to an audit plan, updated quarterly or more often, as needed, that takes into account the bank's risk profile, emerging risks, and issues. 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. Changes to the audit plan should be communicated to the board's audit committee;

(c) Report in writing, conclusions, issues, and recommendations from audit work carried out under the audit plan described in paragraph 3.(b) to the board's audit committee. Internal audit's reports to the audit committee should identify the root cause of any 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 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 effectiveness of the risk governance framework on at least an annual basis.[4] The independent assessment should include a conclusion on the bank's compliance with the standards set forth in these Guidelines and the degree to which the bank's risk governance framework is consistent with leading industry practices;

(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 department 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;

[4] 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.

(g) Develop, attract, and retain talent and maintain staffing levels required to effectively carry out the unit's role and responsibilities, as set forth in paragraphs 3.(a) through 3.(f);

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

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

D. Strategic plan. The Chief Executive Officer should develop 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 impact the bank or that could impact the bank during the period covered by the strategic plan;
2. Articulate an overall mission statement and strategic objectives for the bank, and include an explanation of how the bank will achieve those objectives;
3. Include an explanation of how the bank will update, as necessary, the risk governance framework to account for changes in the bank's risk profile projected under the strategic plan; and

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

E. Risk appetite statement. The bank should have a comprehensive written statement that articulates the 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 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 bank's earnings, capital, and liquidity position. The 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 bank's risk profile jeopardizes the adequacy of its earnings, liquidity, and capital.[5]

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 ensure that front line units do not create excessive risks and, when aggregated across such units, these risks do not exceed the limits established in the bank's risk appetite statement.

G. Risk appetite review, monitoring, and communication processes. The risk governance framework should require:[6]

---

[5] Where possible, 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, banks should establish limits that reasonably reflect the aggregate level of risk that the board of directors and executive management are willing to accept.

[6] With regard to paragraphs 3., 4., and 5. in this paragraph 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 bank's business model, strategy, risk profile, or market conditions.

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 bank's business model, strategy, risk profile, or market conditions;
2. Initial communication and ongoing reinforcement of the bank's risk appetite statement throughout the bank in a manner that ensures all employees align their risk-taking decisions with applicable aspects of the risk appetite statement;
3. Monitoring by independent risk management of the 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 II.C.2.(f) and (g), all at least quarterly.

H. Processes governing risk limit breaches. The 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 bank;
3. Establish protocols for when and how to inform the board of directors, front line unit management, independent risk management, and the OCC of a risk limit breach that takes into account the severity of the breach and its impact on the bank;
4. Include in the protocols established in paragraph 3. 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 bank's size, complexity, and risk profile for effectively identifying, measuring, monitoring, and controlling the bank's concentration 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 ensure that the bank's risk data aggregation and reporting capabilities are appropriate for its size, complexity, and risk profile and support supervisory reporting requirements. Collectively, these policies, procedures, and processes should provide for:

1. The design, implementation, and maintenance of a data architecture and information technology infrastructure that supports the 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. The bank's front line units and independent risk management should incorporate 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. 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. The talent management processes should ensure that:

1. The board of directors or a board committee:

   (i) Hires a Chief Executive Officer and approves the hiring of direct reports of the Chief Executive Officer with the skills and abilities to design and implement an effective risk governance framework;

   (ii) Establishes reliable succession plans for the individuals described in (i) of this paragraph; and

   (iii) Oversees the talent development, recruitment, and succession planning processes for individuals two levels down from the Chief Executive Officer.

2. The board of directors or a board committee:

   (i) Hires one or more Chief Risk Executives and a Chief Audit Executive that possess the skills and abilities to effectively implement the risk governance framework;

   (ii) Establishes reliable succession plans for the individuals described in (i) of this paragraph; and

   (iii) Oversees the talent development, recruitment, and succession planning processes for independent risk management and internal audit.

M. Compensation and performance management programs. The bank should establish and adhere to compensation and performance management programs that meet the requirements of 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;
3. Attract and retain the talent needed to design, implement, and maintain an effective risk governance framework; and
4. 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.

III. STANDARDS FOR BOARD OF DIRECTORS

A. Ensure an effective risk governance framework. Each member of the bank's board of directors has a duty to oversee the bank's compliance with safe and sound banking practices. Consistent with this duty, the board of directors should ensure that the bank establishes and implements 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 changes to the risk governance framework.

B. Provide active oversight of management. The bank's board of directors should actively oversee the bank's risk-taking activities and hold management accountable for adhering to the risk governance framework. In providing active oversight, the board of directors should question, challenge, and when necessary, oppose recommendations and

decisions made by management that could cause the bank's risk profile to exceed its risk appetite or jeopardize the safety and soundness of the bank.

C. Exercise independent judgment. When carrying out his or her duties under III.B., each member of the board of directors should exercise sound, independent judgment.

D. Include independent directors. To promote effective, independent oversight of bank management, at least two members of the board of directors should not be members of the bank's management or the parent company's management.[7]

E. Provide ongoing training to independent directors. To ensure each member of the board of directors has the knowledge, skills, and abilities needed to meet the standards set forth in these Guidelines, the board of directors should establish and adhere to a formal, ongoing training program for independent directors. This program 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.

F. Self-assessments. The 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 170 [Removed]

13. Part 170 is removed.

[7] 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.

Dated: January 10, 2014

//signed//

Thomas J. Curry,
Comptroller of the Currency.