

APPENDIX D TO PART 30—OCC GUIDELINES ESTABLISHING HEIGHTENED STANDARDS FOR CERTAIN LARGE INSURED NATIONAL BANKS, INSURED FEDERAL SAVINGS ASSOCIATIONS, AND INSURED FEDERAL BRANCHES

TABLE OF CONTENTS

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

I. INTRODUCTION

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

2. This appendix establishes minimum standards for the design and implementation of a covered bank's risk governance framework and minimum standards for the covered bank's board of directors in providing oversight to the framework's design and implementation (Guidelines). These standards

are in addition to any other applicable requirements in law or regulation.

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

4. A parent company's and covered bank's risk profiles are substantially the same if, as reported on the covered bank's Federal Financial Institutions Examination Council Consolidated Reports of Condition and Income (Call Reports) for the four most recent consecutive quarters, the covered bank's average total consolidated assets, as calculated according to paragraph I.A. of these Guidelines, represent 95 percent or more of the parent company's average total consolidated assets.<sup>1</sup> A covered bank that does not satisfy this test may submit a written analysis to the OCC for consideration and approval that demonstrates that the risk profile of the parent company and the covered bank are substantially the same based upon other factors not specified in this paragraph.

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

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

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

those components are consistent with the objectives of these Guidelines.

#### A. Scope

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

#### B. Compliance Date

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

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

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

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

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

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

#### C. Reservation of Authority

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

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

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

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

#### D. Preservation of Existing Authority

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

#### E. Definitions

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

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

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

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

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

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

5. *Covered bank* means any bank:

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

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

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

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

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

(ii) Provides operational support or servicing to any organizational unit or function within the covered bank for the delivery of products or services to customers; or

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

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

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

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

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

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

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

8. *Internal audit* means the organizational unit within a covered bank that is designated to fulfill the role and responsibilities outlined in 12 CFR part 30, Appendix A, II.B. Internal audit maintains independence from front line units and independent risk management through the following reporting structure:

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

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

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

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

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

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

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

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

## II. STANDARDS FOR RISK GOVERNANCE FRAMEWORK

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

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

C. *Roles and Responsibilities.* The risk governance framework should include well-defined risk management roles and responsibilities for front line units, independent risk

management, and internal audit.<sup>2</sup> The roles and responsibilities for each of these organizational units should be:

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

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

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

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

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

(e) Develop, attract, and retain talent and maintain staffing levels required to carry out the unit's role and responsibilities effectively,

<sup>2</sup>These roles and responsibilities are in addition to any roles and responsibilities set forth in Appendices A, B, and C to Part 30. Many of the risk management practices established and maintained by a covered bank to meet these standards, including loan review and credit underwriting and administration practices, should be components of its risk governance framework, within the construct of the three distinct units identified herein. In addition, existing OCC guidance sets forth standards for establishing risk management programs for certain risks, e.g., compliance risk management. These risk-specific programs should also be considered components of the risk governance framework, within the context of the three units described in paragraph II.C. of these Guidelines.

tively, as set forth in paragraphs II.C.1.(a) through (d) of these Guidelines;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

### 3. Role and Responsibilities of Internal Audit.

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

(a) Maintain a complete and current inventory of all of the covered bank's material processes, product lines, services, and functions, and assess the risks, including emerging risks, associated with each, which collectively provide a basis for the audit plan described in paragraph II.C.3.(b) of these Guidelines;

(b) Establish and adhere to an audit plan that is periodically reviewed and updated that takes into account the covered bank's risk profile, emerging risks, and issues, and establishes the frequency with which activities should be audited. The audit plan should require internal audit to evaluate the adequacy of and compliance with policies, procedures, and processes established by front line units and independent risk management under the risk governance framework. Significant changes to the audit plan should be communicated to the board's audit committee;

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

(i) A determination of whether the root cause creates an issue that has an impact on one organizational unit or multiple organizational units within the covered bank; and

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

(d) Establish and adhere to processes for independently assessing the design and ongoing effectiveness of the risk governance framework on at least an annual basis. The

independent assessment should include a conclusion on the covered bank's compliance with the standards set forth in these Guidelines;<sup>3</sup>

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

(f) Establish a quality assurance program that ensures internal audit's policies, procedures, and processes comply with applicable regulatory and industry guidance, are appropriate for the size, complexity, and risk profile of the covered bank, are updated to reflect changes to internal and external risk factors, emerging risks, and improvements in industry internal audit practices, and are consistently followed;

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

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

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

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

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

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

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

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

<sup>3</sup>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.

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

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

G. *Risk Appetite Review, Monitoring, and Communication Processes.* The risk governance framework should require:<sup>5</sup>

1. Review and approval of the risk appetite statement by the board of directors or the board's risk committee at least annually or more frequently, as necessary, based on the size and volatility of risks and any material changes in the covered bank's business model, strategy, risk profile, or market conditions;
2. Initial communication and ongoing reinforcement of the covered bank's risk appetite statement throughout the covered bank in a manner that causes all employees to align their risk-taking decisions with applicable aspects of the risk appetite statement;
3. Monitoring by independent risk management of the covered bank's risk profile rel-

ative to its risk appetite and compliance with concentration risk limits and reporting on such monitoring to the board of directors or the board's risk committee at least quarterly;

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

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

H. *Processes Governing Risk Limit Breaches.* A covered bank should establish and adhere to processes that require front line units and independent risk management, in conjunction with their respective responsibilities, to:

1. Identify breaches of the risk appetite statement, concentration risk limits, and front line unit risk limits;
2. Distinguish breaches based on the severity of their impact on the covered bank;
3. Establish protocols for when and how to inform the board of directors, front line unit management, independent risk management, internal audit, and the OCC of a risk limit breach that takes into account the severity of the breach and its impact on the covered bank;
4. Include in the protocols established in paragraph II.H.3. of these Guidelines the requirement to provide a written description of how a breach will be, or has been, resolved; and
5. Establish accountability for reporting and resolving breaches that include consequences for risk limit breaches that take into account the magnitude, frequency, and recurrence of breaches.

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

J. *Risk Data Aggregation and Reporting.* The risk governance framework should include a set of policies, supported by appropriate procedures and processes, designed to provide risk data aggregation and reporting capabilities appropriate for the size, complexity, and risk profile of the covered bank, and to support supervisory reporting requirements. Collectively, these policies, procedures, and processes should provide for:

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

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

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

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

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

K. *Relationship of Risk Appetite Statement, Concentration Risk Limits, and Front Line Unit Risk Limits to Other Processes.* A covered bank's front line units and independent risk management should incorporate at a minimum the risk appetite statement, concentration risk limits, and front line unit risk limits into the following:

1. Strategic and annual operating plans;

2. Capital stress testing and planning processes;

3. Liquidity stress testing and planning processes;

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

5. Decisions regarding acquisitions and divestitures; and

6. Compensation and performance management programs.

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

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

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

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

M. *Compensation and Performance Management Programs.* A covered bank should establish and adhere to compensation and performance management programs that com-

ply with any applicable statute or regulation and are appropriate to:

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

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

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

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

### III. STANDARDS FOR BOARD OF DIRECTORS

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

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

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

D. *Include Independent Directors.* To promote effective, independent oversight of the covered bank's management, at least two members of the board of directors:<sup>6</sup>

<sup>6</sup>This provision does not supersede other regulatory requirements regarding the composition of the Board that apply to Federal

*Continued*

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

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

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

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

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

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

3. Other topics identified by the board of directors.

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

[79 FR 54545, Sept. 11, 2014]

## PART 31—EXTENSIONS OF CREDIT TO INSIDERS AND TRANSACTIONS WITH AFFILIATES

Sec.

31.1 Authority.

31.2 Insider lending restrictions and reporting requirements.

APPENDIX A TO PART 31—INTERPRETATIONS: DEPOSITS BETWEEN AFFILIATED BANKS

APPENDIX B TO PART 31—COMPARISON OF SELECTED PROVISIONS OF PART 31 AND PART 32 (AS OF OCTOBER 1, 1996)

AUTHORITY: 12 U.S.C. 93a, 375a(4), 375b(3), and 1817(k).

SOURCE: 61 FR 54536, Oct. 21, 1996, unless otherwise noted.

savings associations. These institutions must continue to comply with such other requirements.

### §31.1 Authority.

This part is issued by the Comptroller of the Currency pursuant to 12 U.S.C. 93a, 375a(4), 375b(3), 1817(k) and 1817(k), as amended.

[61 FR 54536, Oct. 21, 1996, as amended at 73 FR 22251, Apr. 24, 2008]

### §31.2 Insider lending restrictions and reporting requirements.

(a) *General rule.* A national bank and its insiders shall comply with the provisions contained in 12 CFR part 215.

(b) *Enforcement.* The Comptroller of the Currency administers and enforces insider lending standards and reporting requirements as they apply to national banks and their insiders.

#### APPENDIX A TO PART 31—INTERPRETATIONS: DEPOSITS BETWEEN AFFILIATED BANKS

*a. General rule.* A deposit made by a bank in an affiliated bank is treated as a loan or extension of credit to the affiliate bank under 12 U.S.C. 371c, as this statute is implemented by the Federal Reserve Board's Regulation W, 12 CFR part 223. Thus, unless an exemption from Regulation W is available, these deposits must be secured in accordance with 12 CFR 223.14. However, a national bank may not pledge assets to secure private deposits unless otherwise permitted by law (*see, e.g.*, 12 U.S.C. 90 (permitting collateralization of deposits of public funds); 12 U.S.C. 92a (trust funds); and 25 U.S.C. 156 and 162a (Native American funds)). Thus, unless one of the exceptions to 12 CFR part 223 noted in paragraph b. of this interpretation applies, unless another exception applies that enables a bank to meet the collateral requirements of §223.14, or unless a party other than the bank in which the deposit is made can legally offer and does post the required collateral, a national bank may not:

1. Make a deposit in an affiliated national bank;

2. Make a deposit in an affiliated State-chartered bank unless the affiliated State-chartered bank can legally offer collateral for the deposit in conformance with applicable State law and 12 CFR 223.14; or

3. Receive deposits from an affiliated bank.

*b. Exceptions.* The restrictions of 12 CFR part 223 (other than 12 CFR 223.13, which requires affiliate transactions to be consistent with safe and sound banking practices) do not apply to deposits:

1. Made in an affiliated depository institution or affiliated foreign bank provided that the deposit represents an ongoing, working balance maintained in the ordinary course of