OCC Final Guidelines Establishing Heightened Standards for Certain Large Insured Banking Institutions

Executive Summary

The Office of the Comptroller of the Currency ("OCC" or "agency") adopted guidelines, issued as a new *Appendix D* to *12 CFR part 30* of its safety and soundness regulations, establishing thirteen separate minimum standards for the design and implementation of a risk governance framework ("framework") to manage and control risk-taking activities and six minimum standards for oversight of the framework's design and implementation by boards of directors ("boards"). The final Heightened Standards guidelines are generally consistent with the OCC's proposal[1] released in January 2014, with some modifications made in response to comments received. The guidelines include revisions intended to provide additional clarity and flexibility, as well as avoid the imposition of managerial-type responsibilities on board members.

The guidelines are applicable to "covered banks," which are defined to include insured national banks, insured federal savings associations, and insured federal branches of foreign banks (collectively, "banks") with average total consolidated assets of at least $50 billion. While the guidelines will apply to all banks with average total consolidated assets of at least $50 billion, a bank with average total consolidated assets of less than $50 billion that has either (1) a parent company controlling at least one covered bank or (2) operations determined by the OCC to be highly complex or otherwise present a heightened risk is also classified as a covered bank under the guidelines. These final guidelines supersede the OCC's previous heightened expectations program with respect to covered banks.

As a part of the OCC's ongoing efforts to integrate its regulations with those of the Office of Thrift Supervision, the OCC also adopted final rules and guidelines that integrate *12 CFR parts 30* and *170* by making all of its safety and soundness standards regulations and guidelines under *part 30* applicable to both national banks and federal savings associations and removing the comparable federal savings association regulations and guidelines under *part 170*.

The final rule is effective November 10, 2014. The OCC has established expected compliance dates for the final guidelines under a tiered, phased-in schedule based on a covered bank's average total consolidated assets, outlined in more detail below.

[1] See KPMG Regulatory Practice Letter 14-04.

Key Takeaways

The guidelines include the following modifications and clarifications related to a covered bank's framework:

- Clarification that a covered bank may use its parent company's framework in its entirety and without modification, if the framework meets the guidelines' standards and the risk profiles of both entities are substantially the same (i.e., if the covered bank's average total consolidated assets represent at least 95 percent of the parent company's average total consolidated assets.
  - The guidelines remove the proposed test components contained in the OCC's January 2014 proposal that included total assets under management ("AUM") and total off-balance sheet exposures.
- Clarification that a covered bank that does not meet the substantially the same test may, in consultation with the OCC, incorporate or rely on components of its parent company's frameworks when developing its own framework.
- Increased flexibility for insured federal branches that applies the guidelines in a manner that takes into account the nature, scope, and risk of their activities.

The guidelines include the following modifications and clarifications related to board standards:

- Clarification that, while the OCC expects the board or one of its committees to provide oversight to a covered bank's talent management program, the responsibility for developing and implementing the program rests with the covered bank's management.
- Clarification that the board will not be expected to "ensure," or guarantee, results under a covered bank's framework.
- Clarification that the board may rely on risk assessments and reports prepared by independent risk management and internal audit, and is not prohibited from engaging third-party experts to assist the board in carrying out its duties.
- Increased flexibility for boards in structuring a formal, ongoing training program for directors that includes consideration of the directors' knowledge and experience, as well as the covered bank's risk profile.

Background

In response to the 2008 financial crisis, the OCC developed a set of "heightened expectations," also referred to as the "Get to Strong" principles, to enhance its supervision and strengthen the governance and risk management practices of large national banks ("large banks"). The heightened expectations reflected the OCC's supervisory experience during the financial crisis and addressed certain weaknesses the agency observed in large institutions' governance and risk management practices.

These heightened expectations included the following five standards for large banks:

- The board has a primary fiduciary duty to preserve the "sanctity of the charter" by ensuring that the institution operates in a safe and sound manner;
- A "personnel management program" should ensure appropriate staffing levels, provide for orderly succession, and provide for compensation tools to appropriately motivate and retain talent, while discouraging imprudent risk taking;
- An "acceptable risk appetite" should be defined and communicated across the organization, and should include 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;
- A "reliable oversight program" should be established and include the development and maintenance of strong audit and risk management functions that are consistent with OCC standards and leading industry practices; and
- The board is expected to provide a "credible challenge" to bank management's decision-making, and independent directors, in particular, are expected "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 January 2014, the OCC invited public comment on proposed rules and guidelines addressing: (1) guidelines establishing minimum standards for the design and implementation of a framework for large insured national banks, insured Federal savings associations, and insured Federal branches and minimum standards for boards of directors overseeing the framework of these institutions ("proposed guidelines" or "proposal") and (2) the integration of *12 CFR parts 30* and *170*. The final guidelines supersede the OCC's previous heightened expectations program with respect to covered banks. The OCC states that its examiners will assess covered banks' governance and risk management practices using the guidelines and other existing OCC policy guidance, such as handbooks and bulletins, to identify appropriate practices and certain weaknesses, as well as communicate areas needing improvement to the board and management of covered banks under the OCC's existing supervisory processes.

Description

Appendix D—OCC Guidelines Establishing Heightened Standards for Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches to the OCC's *part 30* safety and soundness regulations establishes minimum standards for the design and implementation of a covered bank's framework to manage and control its risk-taking activities, as well as minimum standards for the covered bank's board in providing oversight to the framework's

design and implementation. These standards are additive to any other requirements in law or regulation.

OCC Definitions

The proposed guidelines defined certain terms, including "bank" (previously defined in the proposal's Scope section), "Chief Audit Executive," "Chief Risk Executive," "front line unit," "independent risk management," "internal audit," "risk appetite," and "risk profile." With the exception of the "front line unit" definition, the OCC adopted these definitions substantially as originally proposed, with certain clarifying and technical changes:

- **Bank** continues to mean any insured national bank, insured federal savings association, or insured federal branch of a foreign bank.
- **Chief Audit Executive** ("CAE") continues to mean an individual who leads internal audit and is one level below the Chief Executive Officer ("CEO") in a covered bank's organizational structure.
- **Chief Risk Executive** ("CRE") continues to mean an individual who leads an independent risk management unit and is one level below the CEO in a covered bank's organizational structure.
  - In response to comments received on the proposed guidelines, the final definition expressly states that a covered bank "may have more than one" CRE. However, a covered bank with multiple, risk-specific CREs should have effective processes for coordinating the activities of all independent risk management units so that they are able to provide an aggregated view of all risks to the CEO and the board or its risk committee.
- **Independent risk management** continues to mean any organizational unit within a covered bank that is independent from front line units and has responsibility for identifying, measuring, monitoring, or controlling aggregate risks.
  - The final definition removes the provision for the CEO to oversee the CRE's (or CREs') day-to-day activities and the provision that the board or its risk committee review and approve any material policies established under the framework, as these policies should be approved by management.
- **Internal audit** continues to mean the organizational unit within a covered bank that is independent from front line units and independent risk management, and is designated to fulfill the role and responsibilities outlined in *12 CFR part 30, Appendix A, II.B*.[2]
  - The final definition clarifies that the board's audit committee or the CEO oversees the CAE's administrative activities, rather than the CAE's day-to-day activities, and that the audit committee reviews and approves internal audit's overall charter and audit plans, rather than all internal audit risk assessments.
- **Risk appetite** continues to mean the aggregate level and types of risk the board and management are willing to assume to achieve the covered bank's strategic objectives and business plan, consistent with applicable capital, liquidity, and other regulatory requirements.
- **Risk profile** continues to mean a point-in-time assessment of the covered bank's risks, aggregated within and across each relevant risk category, using methodologies consistent with the risk appetite statement described in the guidelines.

[2] See *12 CFR part 30, Appendix A—Interagency Guidelines Establishing Standards for Safety and Soundness, II. Operational and Managerial Standards, B. Internal Audit System*.

The guidelines revise the definition of "front line unit" to provide covered banks with some flexibility when identifying and classifying these units and also add a provision that legal services are not ordinarily included in the "front line unit" classification. Key revisions include:

Definition	Proposed guidelines	Final guidelines
Front line unit	Any organizational unit within the bank that: • Engages in activities designed to generate revenue for the parent company or bank; • Provides services, such as administration, finance, treasury, legal, or human resources, to the bank; or • Provides information technology, operations, servicing, processing, or other support to any organizational unit covered by these guidelines.	Any organizational unit or function thereof in a covered bank that is accountable for either credit risk, interest rate risk, liquidity risk, price risk, operational risk, compliance risk, strategic risk, or reputation risk that: • Engages in activities designed to generate revenue or reduce expenses for the parent company or covered bank; • Provides operational support or servicing to any organizational unit or function within the covered bank for the delivery of products or services to customers; or • Provides technology services to any organizational unit or function covered by the guidelines 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.

For the purposes of clarifying the guidelines' scope, the OCC adopted additional definitions for the terms "covered bank," "parent company," and "control" that were not explicitly defined in the proposal:

- **Covered bank** means any bank with average total consolidated assets[3] of (1) at least $50 billion, (2) less than $50 billion, if that bank's parent company controls at least one covered bank, or (3) less than $50 billion, if the OCC determines the bank's operations are highly complex or otherwise present a heightened risk as to warrant the application of these guidelines pursuant to the OCC's reservation of authority.
- **Parent company** means the top-tier legal entity in a covered bank's ownership structure.

[3] The guidelines clarify that "average total consolidated assets" for a covered bank means the average of the covered bank's total consolidated assets, as reported on the covered bank's Federal Financial Institutions Examination Council Consolidated Reports of Condition and Income ("Call Reports"), for the four most recent consecutive quarters. For the 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 ("Consolidated Financial Statements for Bank Holding Companies") to the Federal Reserve Board, or equivalent regulatory report, for the four most recent consecutive quarters.

- A parent company **controls** a covered bank if it (1) owns, controls, or holds with power to vote 25 percent or more of a class of voting securities of the covered bank or (2) consolidates the covered bank for financial reporting purposes.

Scope and Reservation of Authority

The guidelines apply to any bank with average total consolidated assets of at least $50 billion and also apply to any bank with average total consolidated assets less than $50 billion, if its parent company controls at least one covered bank. The OCC states, however, that it reserves the authority to:

- Apply the guidelines, in whole or in part, to a bank that has average total consolidated assets less than $50 billion, if the OCC determines the bank's operations are highly complex or otherwise present a heightened risk that warrants application of the guidelines;
- Extend the time for compliance with the guidelines or modify the guidelines for each covered bank; and
- Determine that compliance with the guidelines should no longer be required for a covered bank. The OCC would generally make this determination if a covered bank's operations are no longer deemed to be highly complex or present a heightened risk, based on a consideration of the complexity of the covered bank's products and services, risk profile, and scope of operations.

Compliance Dates

The guidelines establish a tiered schedule that phases in compliance expectations for covered banks, based on specific asset thresholds:

Covered bank's average total consolidated assets	Expected compliance date
≥ $750 billion as of November 10, 2014	November 10, 2014
At least $100 billion, but less than $750 billion, as of November 10, 2014	Six months from November 10, 2014
At least $50 billion, but less than $100 billion, as of November 10, 2014	Eighteen months from November 10, 2014
< $50 billion, but classified as a covered bank because its parent company controls at least one other covered bank as of November 10, 2014	The same date that the other covered bank should comply with the guidelines
A covered bank that does not come within the scope of the guidelines on November 10, 2014, but subsequently ≥ $50 billion after November 10, 2014	Eighteen months from the as-of date of the bank's most recent Call Report used in the calculation of the average

Leveraging a Parent Company's Risk Governance Framework

The guidelines clarify that a covered bank may use its parent company's framework in its entirety, without modification, if (1) the parent company's framework meets the guidelines' minimum standards, (2) the risk profiles of the parent company and the

covered bank are "substantially the same," and (3) the covered bank has demonstrated, through a documented assessment, that its risk profile and its parent company's risk profile are substantially the same. This assessment should be conducted at least annually, in conjunction with the review and update of the framework performed by independent risk management.

Consistent with the proposal, the guidelines state that a parent company's and covered bank's risk profiles are substantially the same if, as reported on the covered bank's Call Reports for the four most recent consecutive quarters, the covered bank's average total consolidated assets represent at least 95 percent of the parent company's average total consolidated assets. However, the guidelines remove the proposed tests that a covered bank's total AUM and total off-balance sheet exposures represent at least 95 percent of its parent company's total AUM and total off-balance sheet exposures, respectively. The guidelines also provide that a covered bank that does not satisfy the total consolidated assets test may submit a written analysis to the OCC for its consideration and approval that demonstrates the risk profile of its parent company is substantially the same as its own based upon "other factors."

Consistent with the proposal, a covered bank should establish its own framework when the risk profiles of the parent company and the covered bank 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's 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 and management. When the risk profiles of the parent company and the covered bank are not substantially the same, the guidelines clarify that a covered bank may, in consultation with the OCC, incorporate or rely on components of its parent company's framework when developing its own framework, to the extent those components are consistent with the guidelines' objectives.

Standards for a Covered Bank's Risk Governance Framework

Consistent with the proposal, the guidelines establish the following thirteen separate minimum standards for the framework's design and implementation. These minimum standards should include the following:

Risk Governance Framework

A covered bank should establish and adhere to a formal, written framework that is designed by independent risk management and approved by the board or its risk committee. The guidelines add a provision that the framework should include delegations of authority from the board to management committees and executive officers, as well as the risk limits established for material activities. Independent risk management should review and update the 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.

Scope of the Risk Governance Framework

The 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.

Roles and Responsibilities

The framework should include well-defined risk management roles and responsibilities for the three distinct organizational units that the OCC describes as fundamental to the framework's design and implementation: (1) front line units, (2) independent risk management, and (3) internal audit. These organizational units are often referred to as the "three lines of defense" that, in aggregate, should establish an appropriate system to control risk taking.

These organizational units should also keep the board informed of the covered bank's risk profile and risk management practices to allow the board to provide credible challenges to management's recommendations and decisions. In addition, the OCC states that independent risk management and internal audit are expected to have unrestricted access to the board, or a committee thereof, with regard to their risk assessments, findings, and recommendations, that is independent from front line unit management and, when necessary, the CEO, as this unrestricted access is critical to the integrity of the framework.

In carrying out their responsibilities within the framework, front line units, independent risk management, and internal audit may engage the services of external experts to assist them. However, the OCC states that, while this expertise can be useful in supplementing internal expertise and providing perspective on industry practices, organizational units in the covered bank may not delegate their responsibilities under the framework to an external party.

The roles and responsibilities for each of the three lines of defense should be defined as follows:

- **Front line units** should take responsibility and be held accountable by the CEO and the board 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:
  - Assess, on an ongoing basis, the material risks associated with its activities and use these risk assessments as the basis for fulfilling its responsibilities, as set forth in the guidelines, as well as for determining if actions need to be taken to strengthen risk management or reduce risk given changes in the front line unit's risk profile or other conditions;
  - Establish and adhere to a set of written policies that: (1) include front line unit risk limits as discussed in the guidelines and (2) ensure that 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 in the framework;
  - Establish and adhere to procedures and processes, as necessary, to maintain compliance with these policies; and
  - Adhere to all applicable policies, procedures, and processes established by 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:
  - Take primary responsibility and be held accountable by the CEO and the board for designing a comprehensive written framework that meets the

guidelines' standards and is commensurate with the size, complexity, and risk profile of the covered bank;

- 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, as set forth in the 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;
- Establish and adhere to enterprise policies that include concentration risk limits. These 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 framework;
- Establish and adhere to procedures and processes, as necessary, to ensure compliance with these enterprise policies;
- Identify and communicate to the CEO and the board or its risk committee, material risks and significant instances where independent risk management's assessment of risk differs from that of a front line unit, as well as significant instances where a front line unit is not adhering to the framework, including instances when front line units do not meet the standards set forth in the guidelines' roles and responsibilities for front line units; and
- Identify and communicate to the board or its risk committee material risks and significant instances where independent risk management's assessment of risk differs from the CEO, as well as significant instances where the CEO is not adhering to, or holding front line units accountable for adhering to, the framework.

- **Internal audit** should ensure that the covered bank's framework complies with the guidelines' standards and is appropriate for the size, complexity, and risk profile of the covered bank. In carrying out its responsibilities, internal audit should:
  - Maintain a complete and current inventory of all of the covered bank's material processes, product lines, services, and functions, and assess the risks, including emerging risks, associated with each, which collectively provide a basis for the audit plan described below;
  - Establish and adhere to an audit plan that is periodically (rather than quarterly, as originally proposed) reviewed and updated and that takes into account the covered bank's risk profile, emerging risks, and issues, and establishes the frequency with which activities should be audited. 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. Significant changes to the audit plan should be communicated to the board's audit committee;
  - Report in writing, conclusions, material issues, and recommendations from audit work carried out under the audit plan to the board's audit committee. These reports should also identify the root cause of any material issue and include a determination of whether the root cause creates an issue that has an impact on one or more organizational units within the covered 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;

- Establish and adhere to processes for independently assessing the design and ongoing effectiveness of the framework at least annually. The independent assessment should include a conclusion on the covered bank's compliance with the guidelines' standards. The OCC notes that this annual independent assessment may be conducted by internal audit, an external party, or internal audit in conjunction with an external party;
- Identify and communicate to the board's audit committee significant instances where front line units or independent risk management are not adhering to the framework; and
- 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.

In addition to the guidelines' specific roles and responsibilities of each organizational unit, all three lines of defense should do the following:

- Develop, attract, and retain talent and maintain staffing levels required to effectively carry out each organizational unit's role and responsibilities, as set forth in the guidelines;
- Establish and adhere to talent management processes that comply with the covered bank's framework; and
- Establish and adhere to compensation and performance management programs that comply with the covered bank's framework.

Strategic Plan

The CEO 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 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:

- Contain a comprehensive assessment of risks that currently or could have an impact on the covered bank during the period covered by the strategic plan;
- 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;
- Include an explanation of how the covered bank will update, as necessary, the framework to account for changes in the covered bank's risk profile projected under the strategic plan; and
- 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.

Risk Appetite Statement

A covered bank should have a comprehensive written statement that articulates its risk appetite, including qualitative components and quantitative limits, and serves as the basis for the framework.

- 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 to reduce risk before the covered bank's risk profile jeopardizes the adequacy of its earnings, liquidity, and capital.

The OCC notes that, where possible, a covered bank should establish aggregate risk appetite limits that can be disaggregated and applied at the front line unit level. However, where this is not possible, a covered bank should establish limits that reasonably reflect the aggregate level of risk that the board and executive management are willing to accept.

Concentration and Front Line Unit Risk Limits

The 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.

Risk Appetite Review, Monitoring, and Communication Processes

The framework should require:

- Review and approval of the risk appetite statement by the board or its 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;
- 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;
- Monitoring by independent risk management of the covered bank's risk profile relative to its risk appetite and compliance with concentration risk limits, and reporting on such monitoring to the board or its risk committee at least quarterly;
- Monitoring by front line units of compliance with their respective risk limits and reporting to independent risk management at least quarterly; and
- 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 CEO and the board or its risk committee, all at least quarterly.

The OCC notes that, with respect to the monitoring activities of independent risk management and the front line units, 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.

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:

- Identify breaches of the risk appetite statement, concentration risk limits, and front line unit risk limits;
- Distinguish breaches based on the severity of their impact on the covered bank;
- Establish protocols for when and how to inform the board, 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;
- Include in the protocols a 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.

Concentration Risk Management

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

Risk Data Aggregation and Reporting

The framework should include a set of policies, supported by appropriate procedures and processes, designed to provide risk data aggregation ("RDA") and reporting capabilities appropriate for the covered bank's size, complexity, and risk profile and support supervisory reporting requirements. The policies, procedures, and processes should provide for:

- The design, implementation, and maintenance of a data architecture and information technology infrastructure that supports the covered bank's risk aggregation and reporting needs during normal times and times of stress;
- The capturing and aggregating of risk data and reporting of material risks, concentrations, and emerging risks in a timely manner to the board and the OCC; and
- The distribution of risk reports to all relevant parties at a frequency that meets their needs for decision-making purposes.

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

At a minimum, 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:

- 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 and performance management programs.

Talent Management Processes

The 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. Specifically, the board or an appropriate board committee should:

- Appoint a CEO and appoint or approve the appointment of a CAE and one or more CREs with the skills and abilities to carry out their roles and responsibilities within the framework;
- Review and approve a written talent management program that provides for development, recruitment, and succession planning of the CEO, CAE, and CREs, their direct reports, and other potential successors; and
- Require management to assign individuals specific responsibilities within the talent management program and hold those individuals accountable for the program's effectiveness.

Compensation and Performance Management Programs

The covered bank should establish and adhere to compensation and performance management programs that comply with any applicable statute or regulation and are appropriate to:

- Ensure the CEO, front line units, independent risk management, and internal audit implement and adhere to an effective framework;
- 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 them;
- Attract and retain the talent needed to design, implement, and maintain an effective framework; and
- 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.

Standards for Boards of Directors

Consistent with the proposal, the guidelines establish the following six minimum standards for the covered bank's board in providing oversight to the framework's design and implementation:

- **Require an effective framework.** Each member of a covered bank's board should oversee the covered bank's compliance with safe and sound banking practices and require management to establish and implement an effective risk governance framework that meets the guidelines' minimum standards.
  - ➢ The guidelines remove the proposal's language that stated boards have a "duty" to oversee bank compliance, as well as clarify that the board or its risk committee should approve any significant (rather than all, as originally proposed) changes to, as well as monitor compliance with, the framework.
- **Provide active oversight of management.** A covered bank's board should actively oversee the covered bank's risk-taking activities and hold management accountable for adhering to the framework. In providing active oversight, the board 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.
  - ➢ The guidelines' preamble clarifies that the board is not prohibited from engaging third-party experts to assist it in carrying out its duties.

- **Exercise independent judgment.** Board members are expected to exercise sound, independent judgment when providing active oversight.
- **Include independent directors.** Board membership should include at least two independent directors that: (1) are not officers or employees of the parent company or covered bank, either currently or during the previous three years, (2) are not immediate family members of a person who is, or has been within the last three years, an executive officer of the parent company or covered bank, and (3) meet the qualifications of an independent director under the listing standards of a national securities exchange.
- **Provide ongoing training to all directors.** The board should establish and adhere to a formal, ongoing training program for all of its directors that considers the directors' knowledge and experience, as well as the covered bank's risk profile. The program should include 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.
- **Self-assessments.** A covered bank's board should conduct an annual self-assessment that includes an evaluation of its effectiveness in meeting the standards established for the board in the guidelines.

Enforcement

The OCC is adopting the guidelines pursuant to *Section 39* of the *Federal Deposit Insurance Act*, which authorizes the OCC to prescribe safety and soundness standards in the form of regulations or guidelines. Under *Section 39*, if a bank fails to meet a standard prescribed by regulation, the OCC must require the bank to submit a plan specifying the steps it will take to comply with the standard. However, if the OCC were to determine that a covered bank failed to meet the guidelines' standards, the OCC has the discretion to require the submission of such a plan.

The OCC states that its decisions to issue the Heightened Standards as guidelines, as opposed to regulations, will provide the agency with supervisory flexibility to pursue the most appropriate course of action that takes a covered bank's specific circumstances into account if it fails to meet one or more of the guidelines' standards, as well as its self-corrective and remedial responses.

Commentary

The final Heightened Standards guidelines provide greater certainty to covered banks about the OCC's risk management expectations, while still providing for some flexibility in their interpretation, and will likely improve examiners' ability to assess covered bank compliance with the standards. As expected, the guidelines "hardwire" the heightened expectations program into the OCC examination process and compliment certain final provisions of the *Section 165* rulemaking[4] under the *Dodd-Frank Wall Street Reform and Consumer Protection Act* with respect to a covered bank's: (1) strategic planning, (2) product and service risk management processes, (3) stress testing processes that address earnings, capital, and liquidity, (4) enhanced requirements for risk and audit committees, and (5) additional risk management obligations.

The final guidelines address industry comments and offer some relief for boards by removing the proposed language that its members should "ensure," or guarantee, results under the framework. However, boards will still be expected to significantly expand their oversight activities under the guidelines, including the expectation that members provide a "credible challenge" to bank managements' decision making. Although the guidelines' preamble states that boards will not be expected to evidence opposition to management during each board meeting, but rather only as necessary, covered banks will still need to consider how best to document their processes in order to demonstrate that this challenge is both "credible" and occurring under the appropriate circumstances.

The removal of the AUM and off-balance sheet exposure requirements from the "substantially the same risk profile" test may also provide some relief for covered banks seeking to use their parent companies' entire frameworks. A covered bank meeting the 95 percent threshold for average total consolidated assets, however, will still need to establish an annual process that assesses and documents the equivalency of its risk profile to that of its parent company. The retention of the 95 percent asset threshold, while less problematic to calculate under current regulatory reporting requirements than AUM and off-balance sheet exposures, will likely represent a high bar for some banks to meet, thus necessitating the establishment of a separate and distinct framework. Although the guidelines provide that a covered bank not satisfying this test may submit a written analysis to the OCC demonstrating its risk profile is substantially the same as its parent's based upon "other factors," it remains unclear what other criteria will ultimately be considered an acceptable substitute.

In addition, while large banks covered by the OCC's "Get to Strong" program have been actively working with their examiners for the past few years and are therefore likely relatively well positioned to meet the guidelines' standards, mid-size covered banks may have significant work ahead in order to meet the minimum standards, including establishing and implementing the standards for separate organizational units, building the necessary internal controls structure, and further strengthening their RDA and reporting capabilities. These banks will also likely need to strengthen the composition and oversight of their board and top tier management in a highly

[4] See KPMG Regulatory Practice Letter 14-07.

competitive environment where talent meeting the requisite qualifications will be in great demand.

Lastly, covered banks and their parent companies will need to assess the degree of regulatory correlation between the OCC's Heightened Standards and the Federal Reserve Board's Enhanced Prudential Standards embodied in *Section 165* in order to efficiently leverage their resources and meet these supervisory expectations. Covered domestic banks with foreign operations, as well as foreign banks with insured federal branches, will also need to consider similar heightened standards being promulgated by foreign "host country" supervisors that will likely further address, among other things, board oversight, risk culture, the governance framework, risk assessments, and escalation.

This is a publication of KPMG's Financial Services Regulatory Risk Advisory Practice and the Americas' Financial Services Regulatory Center of Excellence

For additional information, please contact:
Hugh Kelly, Principal: hckelly@kpmg.com
Philip Aquilino, Managing Director: paquilino@kpmg.com
Ken Albertazzi, Principal, kalbertazzi@kpmg.com
Pam Martin, Managing Director: pamelamartin@kpmg.com
David Stone, Director: dstone2@kpmg.com

Author: Lisa Newport, Assoc. Director, Americas' Financial Services Regulatory Center of Excellence: lisanewport@kpmg.com

Earlier editions are available at:
www.kpmg.com/us/regulatorypracticeletters