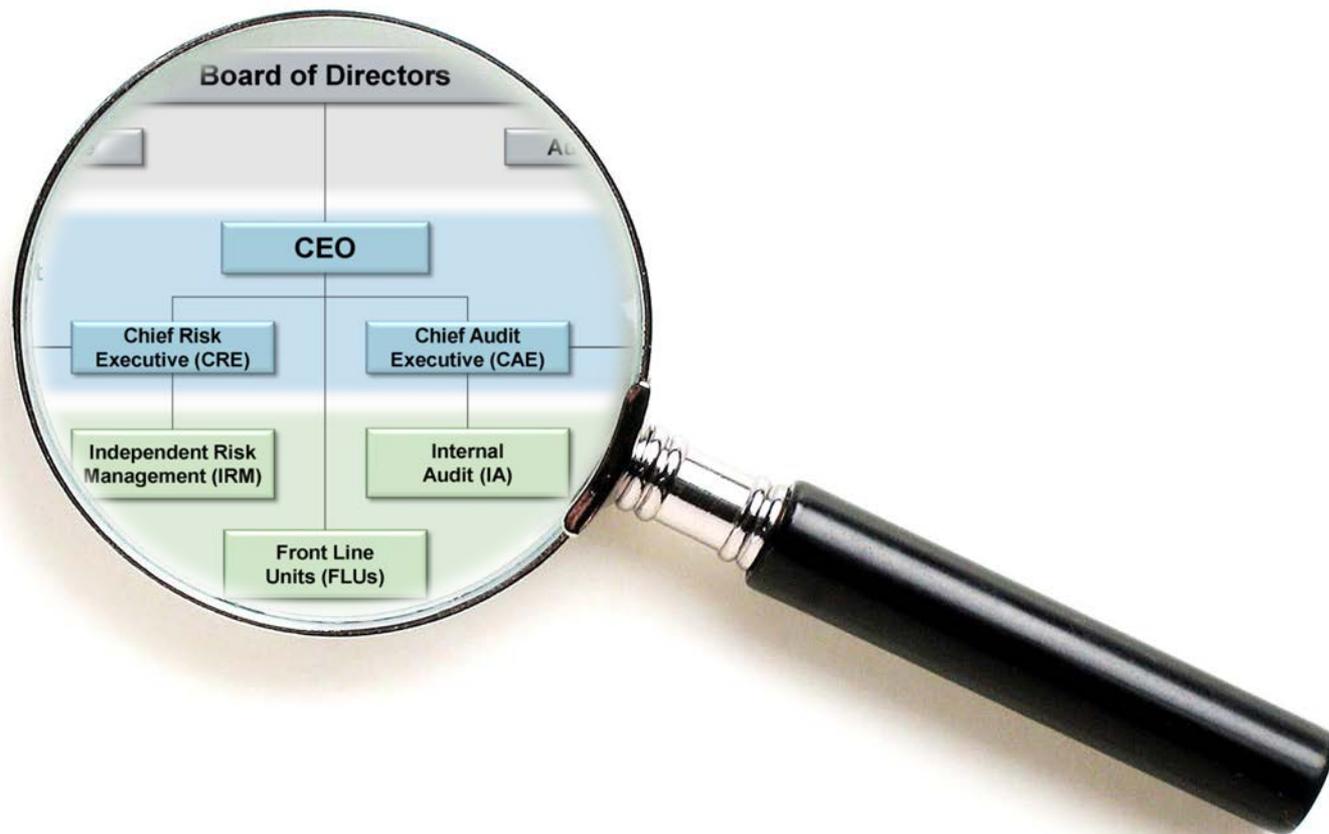


# Risk Governance

## Visual Memorandum on Guidelines Proposed by the OCC



January 29, 2014

# Davis Polk

Davis Polk & Wardwell LLP

© 2014 Davis Polk & Wardwell LLP | 450 Lexington Avenue | New York, NY 10017

Notice: This publication, which we believe may be of interest to our clients and friends of the firm, is for general information only. It is not a full analysis of the matters presented and should not be relied upon as legal advice. If you have received this email in error, please notify the sender immediately and destroy the original message, any attachments thereto and all copies. Refer to the firm's [privacy policy](#) located at [davispolk.com](#) for important information on this policy. Please consider adding Davis Polk to your Safe Senders list or adding [dpwmail@davispolk.com](mailto:dpwmail@davispolk.com) to your address book.

Unsubscribe: If you would rather not receive these publications, please respond to this email and indicate that you would like to be removed from our distribution list.

# Table of Contents

Click on an item to go to that page 

---

<b><u>I. Introduction to Risk Governance and the OCC’s Guidelines</u></b>	5
<u>Overview of the OCC’s Risk Governance Guidelines</u>	6
<u>Risk Governance: At the Center of Effective Risk Management and Regulatory Compliance</u>	8
<u>Roadmap to the OCC’s Risk Governance Guidelines</u>	9
<u>OCC’s Heightened Expectations Program</u>	10
<u>OCC’s Risk Governance Guidelines: Which Banking Organizations Are Affected?</u>	13
<u>Enforcement of the OCC’s Risk Governance Guidelines (Including Flowchart)</u>	15
<b><u>II. Risk Governance Framework: Structure and Responsibilities</u></b>	17
<u>Risk Governance Structure</u>	18
<u>Board Composition Requirements: Two Independent Directors</u>	20
<u>Board of Directors Responsibilities – Checklist</u>	21
<u>CEO Responsibilities – Checklist</u>	29
<u>Chief Risk Executive and Chief Audit Executive Responsibilities</u>	32

# Table of Contents *(cont.)*

Click on an item to go to that page 

<a href="#"><u>Structure of the Three Lines of Defense</u></a>	33
<a href="#"><u>Front Line Unit Responsibilities – Checklist</u></a>	36
<a href="#"><u>Independent Risk Management Responsibilities – Checklist</u></a>	39
<a href="#"><u>Internal Audit Responsibilities – Checklist</u></a>	43
<b><a href="#"><u>III. Risk Governance Framework: Policies, Procedures, Processes and Programs</u></a></b>	47
<a href="#"><u>Written Risk Governance Framework</u></a>	48
<a href="#"><u>Written Strategic Plan</u></a>	50
<a href="#"><u>A Bank’s Risk Profile</u></a>	51
<a href="#"><u>Written Risk Appetite Statement</u></a>	52
<a href="#"><u>Concentration and Front Line Unit Risk Limits</u></a>	57
<a href="#"><u>Risk Appetite Monitoring and Communication Processes</u></a>	59
<a href="#"><u>Processes Governing Risk Limit Breaches</u></a>	60
<a href="#"><u>Risk Data Aggregation and Reporting</u></a>	61

# Table of Contents *(cont.)*

Click on an item to go to that page 

<a href="#"><u>Relationship of Risk Appetite Statement, Concentration Limits and Front Line Unit Risk Limits to Other Processes</u></a>	63
<a href="#"><u>Audit Plan</u></a>	64
<a href="#"><u>Talent Management Processes</u></a>	66
<a href="#"><u>Compensation and Performance Management Programs</u></a>	67
<b><a href="#"><u>IV. Risk Governance Framework: Relationship Between Subsidiary Bank's and Parent Company's Risk Governance Frameworks</u></a></b>	68
<a href="#"><u>A Bank Must Generally Develop Its Own Risk Governance Framework</u></a>	69
<a href="#"><u>Using Components of Parent Company's Risk Governance Framework</u></a>	70
<a href="#"><u>OCC's Risk Governance Guidelines and Dodd-Frank Enhanced Risk Management Standards for Large U.S. BHCs and Large FBOs</u></a>	71
<b><a href="#"><u>Davis Polk Contacts</u></a></b>	73

# I. Introduction to Risk Governance and the OCC's Guidelines

# Overview of the OCC's Risk Governance Guidelines

- Since the financial crisis, the OCC has developed a set of heightened expectations to enhance its supervision and strengthen the risk management practices and governance of the largest national banks. See [page 10](#) (OCC's heightened expectations).
- In January 2014, the OCC proposed a set of **enforceable** and specific risk governance guidelines to formalize those heightened expectations for national banks and federal savings associations (banks) with **≥ \$50 billion** in total consolidated assets.
- The risk governance guidelines would set new, and much higher, minimum standards for:
  - The design and implementation of a bank's **own risk governance framework**; and
  - The **oversight by the bank's board of directors** of the bank's risk governance framework.
- **State Banks:** State banks that are not subject to the OCC's proposed risk governance guidelines should still pay attention because the same or similar principles will likely be applied by the Federal Reserve and the FDIC to large state member and non-member banks.
- **Mid-size Banks:** OCC may apply the risk governance guidelines to a < \$50 billion bank if it determines that the bank's operations are highly complex or otherwise present a heightened risk.

# Regulatory Focus on Risk Governance

- The OCC's risk governance guidelines represent the latest in a trend of rulemakings and supervisory pronouncements that focus on a banking organization's risk management framework and corporate governance structure as well as the responsibilities of the board of directors, senior management and the three lines of defense (*i.e.*, front line units, independent risk management and internal audit).
- This trend will continue in the foreseeable future as:
  - The Federal Reserve implements the Dodd-Frank Act's enhanced risk management standards for large U.S. bank holding companies (BHCs), large foreign banking organizations (FBOs) and systemically important nonbank financial companies;
  - Banking organizations design and implement comprehensive compliance and risk governance programs for the Volcker Rule, Dodd-Frank liquidity risk management standards, capital planning and stress testing, the changing derivatives regulatory landscape as well as other important legal and regulatory developments; and
  - The Federal Reserve and FDIC apply similar risk governance principles to large state banks and all three U.S. banking agencies apply some or all of these principles, over time, to mid-size banking organizations.
- In short, risk governance is here to stay and its importance will only increase over time.

# Risk Governance: At the Center of Effective Risk Management and Regulatory Compliance



# Roadmap to the OCC's Risk Governance Guidelines

- **Structure of the risk governance framework**, including the relationship between the board of directors, senior management and the three lines of defense. See [page 18](#).
- **Composition of the board of directors**, including the requirement to have at least 2 independent directors who are not part of the bank's or parent company's management. See [page 20](#).
- **Board of directors responsibilities** under the risk governance framework. See [page 21](#).
- **Senior management responsibilities** under the risk governance framework. See [page 29](#).
- **Responsibilities of the three lines of defense** that are fundamental to the design and implementation of the risk governance framework. See [page 33](#).
- **Written risk governance framework and strategic plan**. See [page 48](#).
- **Written risk appetite statement** that includes both qualitative components and quantitative limits and serves as a basis for the risk governance framework. See [page 52](#).
- **Concentration and front line unit risk limits and processes**. See [page 57](#).
- **Talent management processes, compensation and performance management programs** and other key aspects of the risk governance framework. See [page 66](#).
- **Relationship between bank's and parent company's risk governance frameworks**. See [page 68](#).
- **OCC's enforcement of the risk governance guidelines**. See [page 15](#).

# OCC's Heightened Expectations Program

- Since the financial crisis, the OCC has developed a set of heightened expectations to enhance its supervision and strengthen the risk management practices and governance of the largest national banks.
  - **2010:** OCC began communicating these heightened expectations informally to banks in its large bank supervision program through its supervisory function.\*
  - **Late 2011:** OCC began applying the heightened expectations standards to federal savings associations in the large bank supervision program after assuming supervisory responsibility for these institutions from the OTS pursuant to the Dodd-Frank Act.
  - **2012:** OCC began examining each large bank for compliance with the expectations, including documenting its conclusions in the OCC's Report of Examination to reflect each bank's progress in complying with the expectations.
  - **Present:** OCC examiners meet with each large institution's management team on a quarterly basis to discuss its progress towards meeting the OCC's heightened expectations.
  - **Mid-size Banks:** The OCC has also applied aspects of the heightened expectations to banks in its mid-size bank supervision program.\*

\* For supervisory purposes, the OCC designates each national bank and federal savings association as a large, mid-size or community bank. This designation is based on the bank's asset size and the presence or absence of other special factors that affect its risk profile and complexity.

# OCC's Heightened Expectations Program: Five Heightened Expectations

- **1. Preserving the sanctity of the charter:** One of the primary fiduciary duties of a bank's board of directors is to ensure that the bank operates in a safe and sound manner.
  - The 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.
- **2. Maintaining 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.
- **3. Defining and communicating an acceptable risk appetite** across the banking 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 bank.

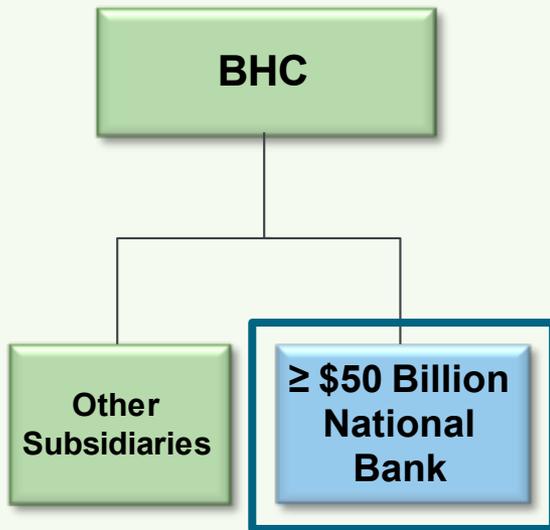
# OCC's Heightened Expectations Program:

## Five Heightened Expectations *(cont.)*

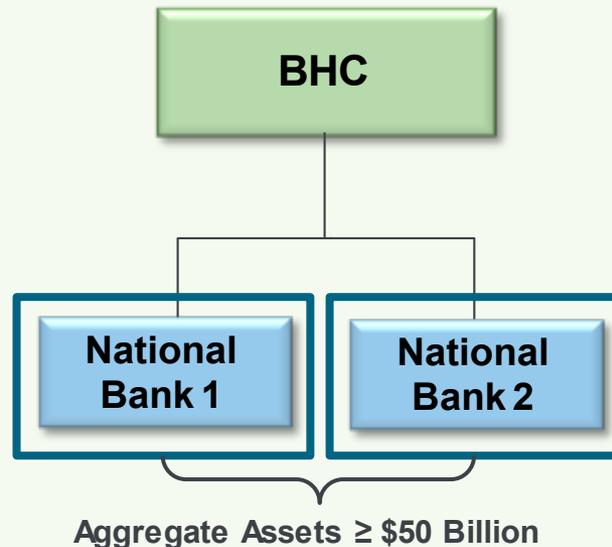
- **4. Maintaining reliable oversight programs**, including the development and maintenance of strong audit and risk management functions.
  - Banks should compare the performance of their audit and risk management functions to the OCC's standards and leading industry practices and take appropriate action to address material gaps.
- **5. Board of directors providing a credible challenge to bank management's decision-making.**
  - Independent directors should acquire a thorough understanding of a bank's risk profile and use this information to ask probing questions of management and ensure that senior management prudently addresses risks.

# OCC's Risk Governance Guidelines: Which Banking Organizations Are Affected?

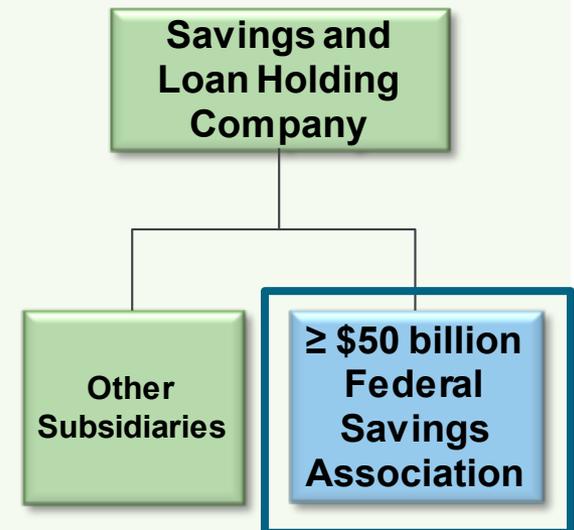
- The OCC's proposed risk governance guidelines would apply to a broader group of banks than those currently subject to the OCC's heightened expectations program.



The proposed risk governance guidelines would apply to a  $\geq$  \$50 billion national bank.

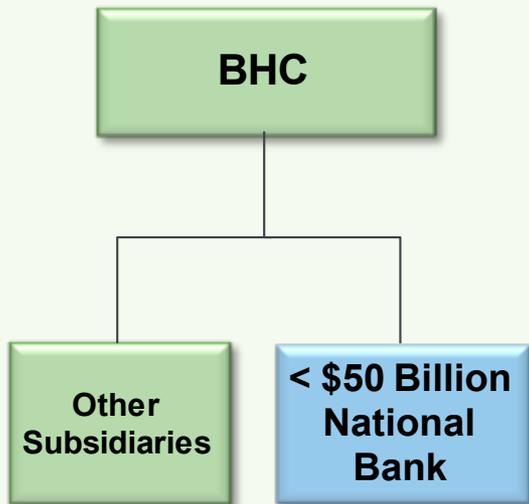


The OCC stated that the proposed risk governance guidelines would generally apply to a  $<$  \$50 billion bank if the **aggregate assets** of all banks owned by its parent company is  $\geq$  \$50 billion.

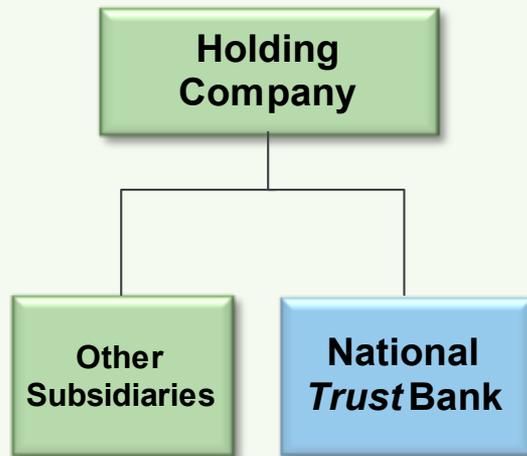


The OCC's proposed risk governance guidelines would apply to a  $\geq$  \$50 billion federal savings association.

# OCC's Risk Governance Guidelines: Which Banking Organizations *May* Be Affected?

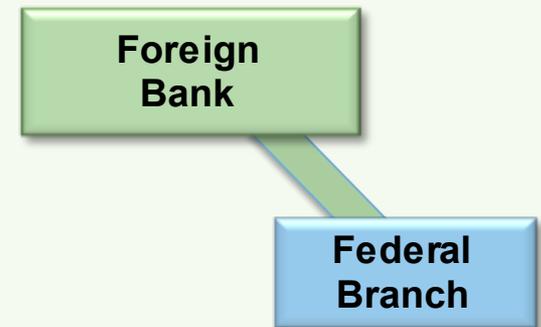


**OCC Discretion:** The OCC **may** apply the proposed risk governance guidelines to a < \$50 billion bank if the OCC determines that the bank's operations are highly complex or otherwise present a heightened risk.



The OCC is considering whether to apply the provisions in the proposed risk governance guidelines to **uninsured** entities, such as national trust banks.

OCC examiners currently are informally applying certain aspects of the heightened expectations to select uninsured entities.



The OCC's proposed risk governance guidelines would apply to a  $\geq$  \$50 billion **insured** federal branch of a foreign bank.

The OCC is considering whether to apply the proposed risk governance guidelines to large uninsured federal branches of foreign banks.

Currently, no federal branch of a foreign bank, insured or uninsured, is  $\geq$  \$50 billion.

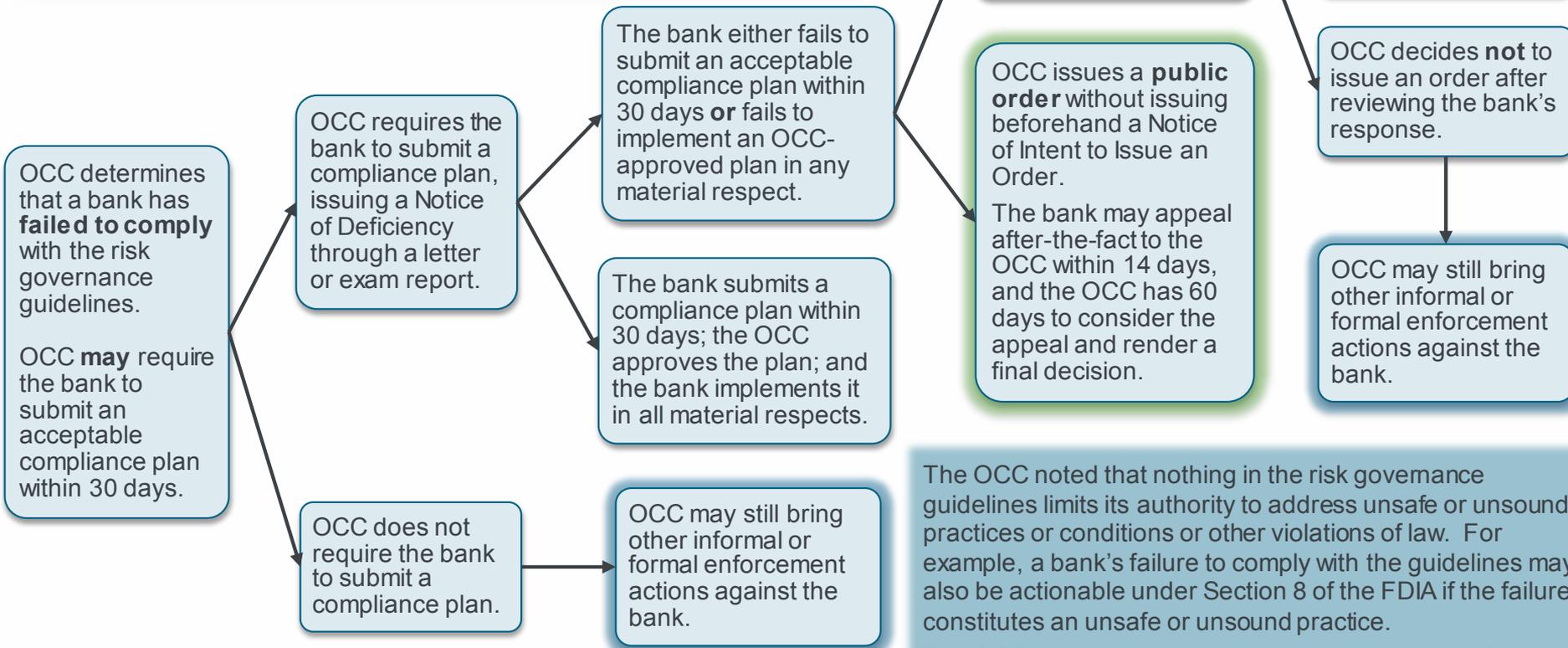
# Enforcement of the OCC's Risk Governance Guidelines

- **Enforcement is a key reason behind the formalization of the OCC's heightened expectations into specific guidelines.**
- The OCC is proposing the risk governance guidelines pursuant to Section 39 of the Federal Deposit Insurance Act (FDIA).
- Section 39 authorizes the OCC to prescribe safety and soundness standards in the form of a regulation or guideline and provides different enforcement procedures depending on whether a bank violates a standard issued by regulation or guideline.
  - **Regulation:** If a bank fails to meet a standard prescribed by regulation, then the OCC **must** require the bank to submit a compliance plan specifying the steps it will take to comply with the relevant standard.
  - **Guideline:** If a bank fails to meet a standard prescribed by guideline, the OCC **has discretion** to decide whether to require the submission of a compliance plan.
- **Order:** Under Section 39, either regulation or guideline ultimately may be enforced by an order.
  - Orders are formal, **public** documents that may be enforced in a federal district court or through the assessment of civil money penalties.
- **Flexibility:** According to the OCC, issuing the risk governance standards as guidelines rather than as a regulation provides it with the flexibility to pursue the course of action that is most appropriate given the specific circumstances of a bank's noncompliance and its self-corrective and remedial responses.

# Section 39 Enforcement Procedures Flowchart

Under Section 39 of the FDIA, the OCC's risk governance guidelines can ultimately be enforced by a **public order**.

In addition to ordering a bank to correct noncompliance, the OCC is authorized under Section 39 to impose restrictions on asset growth, require a bank to increase its tangible equity to assets ratio or limit the interest rate the bank pays on deposits. The OCC *must* impose one or more of these restrictions if the bank has experienced "extraordinary growth" during the previous 18 months.



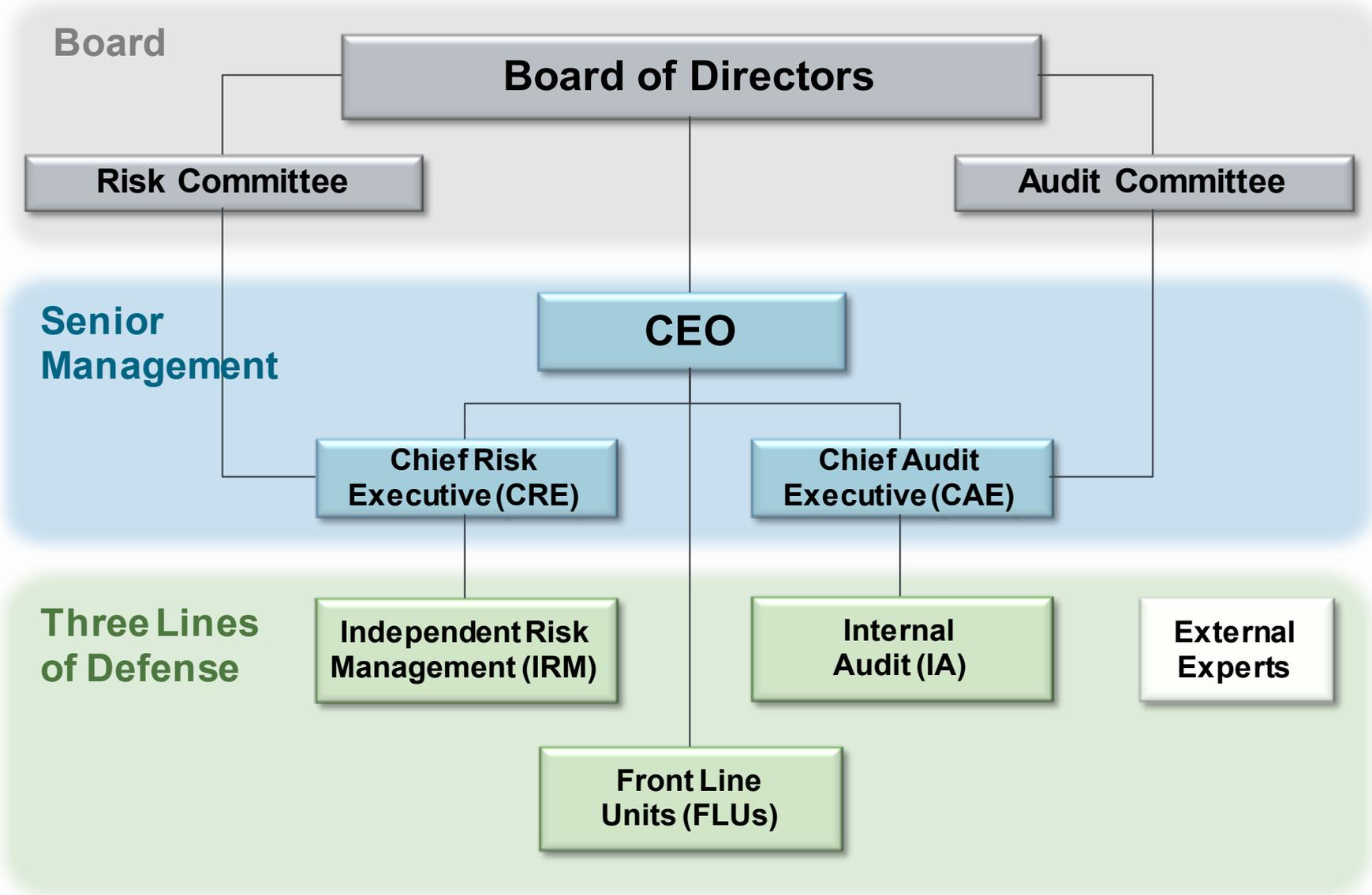
The OCC noted that nothing in the risk governance guidelines limits its authority to address unsafe or unsound practices or conditions or other violations of law. For example, a bank's failure to comply with the guidelines may also be actionable under Section 8 of the FDIA if the failure constitutes an unsafe or unsound practice.

The OCC noted that it may take action pursuant to Section 39 independently of, in conjunction with, or in addition to any other enforcement action available to the OCC.

## II. Risk Governance Framework: Structure and Responsibilities

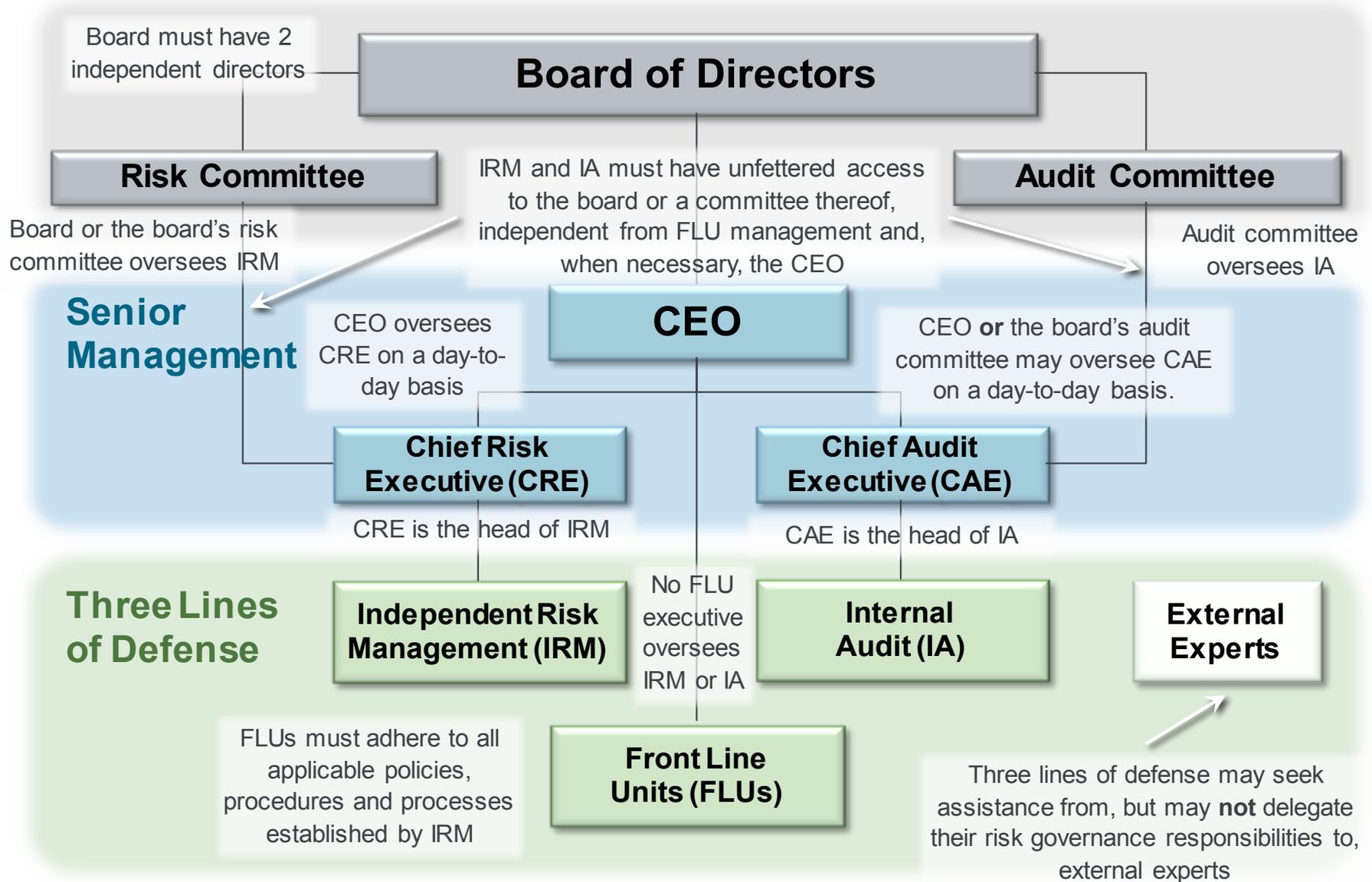
# Risk Governance Structure

The OCC's risk governance guidelines specify the following risk governance structure:



# Key Features of Risk Governance Structure

This visual highlights some of the key features of the risk governance structure:



# Board Composition Requirements: Two Independent Directors

- The OCC's risk governance guidelines provide that:
  - At least **2** members of the bank's board of directors should **not** be members of the bank's management or the parent company's management.\*
- In addition, to the extent a bank's independent directors are also members of the parent company's board of directors, 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.
- A number of large national banks already satisfy the 2 independent directors requirement.

\* This requirement does not supersede other regulatory requirements regarding the composition of the board of directors that apply to federal savings associations, which must continue to comply with such other requirements.

# Board of Directors Responsibilities – Checklist

- Ensure an Effective Risk Governance Framework:** Each member of the 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 in the OCC’s risk governance guidelines.
  - Written Risk Governance Framework:** The board or the board’s risk committee must approve the written risk governance framework, any changes to the framework and any material policies established under the framework. See [page 48](#).
  - Strategic Plan:** The board should evaluate and approve the strategic plan and monitor management’s efforts to implement it at least annually. See [page 50](#).
  - Risk Appetite Statement:** The board or the board's risk committee must review and approve the risk appetite statement 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. See [page 52](#).
  - Safe and Sound Risk Culture:** The board should help promote a safe and sound risk culture by setting an appropriate tone at the top. See [page 54](#).

## Board of Directors Responsibilities – Checklist *(cont.)*

- Provide Active Oversight of Management:** The board of directors should **actively** oversee the bank’s risk-taking activities and hold management accountable for adhering to the risk governance framework.\*
  - The board 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 bank’s safety and soundness.
  - The board should **hold FLUs accountable** for, among other things, appropriately assessing and effectively managing all of the risks associated with FLUs’ activities.
  - The board should **hold IRM accountable** for, among other things, designing a comprehensive written governance framework that meets the risk governance guidelines and is commensurate with the size, complexity and risk profile of the bank.

\* *E.g.*, 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 risk governance framework. In those situations, the OCC expects the board of directors to take action to hold the appropriate party, or parties, accountable.

# Board of Directors Responsibilities – Checklist *(cont.)*

## Oversight of CRE and IRM

- Appointment, Removal and Compensation:** The board or the board's risk committee must approve all decisions regarding the appointment or removal of the CRE and annual compensation and salary adjustment of the CRE.
- Communications from CRE:** The board or the board's risk committee receives communications from the CRE on the results of IRM's risk assessments and activities, and other matters that the CRE determines are necessary.
- IRM Inquiries:** The board or the board's risk committee must make appropriate inquiries of management or the CRE to determine whether there are scope or resource limitations that impede the ability of IRM to execute its responsibilities.

# Board of Directors Responsibilities – Checklist *(cont.)*

## Oversight of CAE and IA

- Appointment, Removal and Compensation:** The board's audit committee must approve all decisions regarding the appointment or removal of the CAE and annual compensation and salary adjustment of the CAE.
- Charter, Risk Assessments and Audit Plans:** The board's audit committee must review and approve IA's overall charter, risk assessments and audit plans.  
See [page 64](#) (audit plan).
- Communications from CAE:** The board's audit committee receives communications from the CAE on the results of IA's activities or other matters that the CAE determines are necessary.
- IA Inquiries:** The board's audit committee makes appropriate inquiries of management or the CAE to determine whether there are scope or resource limitations that impede the ability of IA to execute its responsibilities.

# Board of Directors Responsibilities – Checklist *(cont.)*

- Support for IRM and IA:** According to the OCC, in order for the risk governance framework to be effective, IRM and IA must have the stature needed to effectively carry out their respective responsibilities. The board of directors demonstrates support for IRM and IA by:
  - Ensuring that they have the resources needed to carry out their responsibilities; and
  - Relying on the work of IRM and IA when carrying out the board's oversight responsibilities.
  
- Exercise Independent Judgment:** When carrying out active oversight of management, **each member** of the board of directors 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.

# Board of Directors Responsibilities – Checklist *(cont.)*

- Talent Management:** The board or a committee thereof must:
  - Hire a CEO and approve the hiring of direct reports of the CEO, including the CRE and CAE, with the skills and abilities to design and implement an effective risk governance framework.
  - Establish reliable succession plans for the CEO and his or her direct reports, including the CRE and CAE.
  - Oversee the talent development, recruitment and succession planning processes for individuals two levels down from the CEO.
  - Oversee the talent development, recruitment and succession planning processes for IRM and IA.

## Board of Directors Responsibilities – Checklist *(cont.)*

- 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 the proposed risk governance guidelines, the board should establish and adhere to a formal, ongoing training program for independent directors.
  - The program should include training on:
    - Complex products, services, lines of business and risks that have a significant impact on the bank;
    - Laws, regulations and supervisory requirements applicable to the bank; and
    - Other topics identified by the board.
  - OCC examiners will evaluate each director's knowledge and experience, as demonstrated in their written biography and discussions with examiners.

# Board of Directors Responsibilities – Checklist *(cont.)*

- Annual Self-Assessments.** The board of directors should conduct an annual self-assessment that includes an evaluation of its effectiveness in meeting the OCC’s risk governance guidelines. The self-assessment:
  - 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, *e.g.*, changing:
    - Board composition and structure;
    - Meeting frequency and agenda items;
    - Board report design or content;
    - Ongoing training program design or content; or
    - Other board processes and procedures.

# CEO Responsibilities – Checklist

- Written Risk Governance Framework:** Develop the bank’s written risk governance framework. See [page 48](#).
- Strategic Plan:** With input from the three lines of defense, develop a written strategic plan which articulates a comprehensive assessment of risks facing the bank and an explanation of the bank’s mission and strategic objectives. See [page 50](#).
- Risk Appetite Statement:** Develop the bank’s risk appetite statement, which must include both qualitative components and quantitative limits. See [page 52](#).
- Safe and Sound Risk Culture:** Help promote a safe and sound risk culture by setting an appropriate tone at the top. See [page 54](#).
- Oversight of FLUs and IRM:** Oversee FLUs and IRM to ensure their compliance with requirements under the risk governance guidelines.
  - Hold FLUs and IRM accountable for failure to comply with the risk governance guidelines.

# CEO Responsibilities – Checklist *(cont.)*

- Oversight of CRE:** Oversee day-to-day activities of CRE, including:
  - Resolving disagreements between FLUs and IRM that cannot be resolved by the CRE and FLU executives.
  - Oversight of **(1)** budgeting and management accounting, **(2)** human resources administration, **(3)** internal communications and information flows and **(4)** administration of IRM policies and procedures.
- Oversight of CAE:** Unless the CAE reports to the board’s audit committee,\* oversee day-to-day activities of CAE, including:
  - Oversight of **(1)** budgeting and management accounting, **(2)** human resources administration, **(3)** internal communications and information flows and **(4)** administration of IA policies and procedures.

\* At some banks, the board’s audit committee may assume the CEO’s responsibilities for overseeing the CAE’s day-to-day activities. This is an acceptable governance structure under the OCC’s risk governance guidelines.

# CEO Responsibilities – Checklist *(cont.)*

- Support for IRM and IA:** According to the OCC, in order for the risk governance framework to be effective, IRM and IA must have the stature needed to effectively carry out their respective responsibilities. The CEO and FLUs demonstrate support for IRM and IA by:
  - Welcoming credible challenges from IRM and IA; and
  - Including IRM and IA in policy development, new product and service deployment, changes in strategy and tactical plans, and organizational and structural changes.

# Chief Risk Executive and Chief Audit Executive Responsibilities

## CRE Responsibilities\*

- Leadership of IRM:** Lead IRM in fulfilling its responsibilities under the risk governance framework. See [page 39](#) (IRM responsibilities).
- Communicate to Board of Directors:** Provide information to the board of directors or board's risk committee regarding the results of IRM's risk assessments and activities, and other matters that the CRE determines are necessary.

## CAE Responsibilities

- Leadership of IA:** Lead IA in fulfilling its responsibilities under the risk governance framework. See [page 43](#) (IA responsibilities).
- Communicate to Board of Directors:** Provide information to the board's audit committee regarding the results of IA's activities or other matters that the CAE determines are necessary.

\* **Multiple CREs:** Many banks designate one CRE, such as a chief risk officer, to oversee all IRM units, while other banks designate multiple risk-specific CREs. A bank that designates multiple CREs should have a process for coordinating the activities of all IRM units so they can provide an aggregated view of risks to the CEO and the board of directors or the board's risk committee.

# Structure of the Three Lines of Defense:

## Front Line Units (FLUs)

- **Definition:** FLU is any organizational unit within the bank that engages in any of the following:
  - **Revenue Generation:** Engages in activities designed to generate revenue for the parent company or bank.
  - **Provision of Services:** Provides services, such as administration, finance, treasury, legal or human resources, to the bank.
  - **Provision of Support:** Provides information technology, operations, servicing, processing or other support to any of the above.
- **Risk Creation:** According to the OCC, by engaging in any of the above activities, FLUs create risks for the bank.
- **Accountability:** FLUs should be held accountable by the CEO and the board of directors for compliance with the risk governance guidelines. See [page 36](#) (FLU responsibilities).
- **No Oversight of IRM or IA:** No FLU executive should oversee IRM or IA.

# Structure of the Three Lines of Defense: Independent Risk Management (IRM)

- **Definition:** IRM is any organizational unit within the bank that has responsibility for identifying, measuring, monitoring or controlling aggregate risks.
  - At some banks, IRM is referred to as “risk organization” or “enterprise risk management.”
- **Independence:** IRM maintains independence from FLUs through the following reporting structure:
  - The board of directors or the board’s risk committee reviews and approves the risk governance framework and any material policies established under it.
  - The board or the board’s risk committee approves all decisions regarding the appointment or removal of the CRE (the head of IRM) and approves the annual compensation and salary adjustment of the CRE.
  - The CEO oversees the CRE’s day-to-day activities.
  - No FLU executive oversees IRM.
- **Accountability:** IRM should be held accountable by the CEO and the board of directors for compliance with the risk governance guidelines. See [page 39](#) (IRM responsibilities).

# Structure of the Three Lines of Defense:

## Internal Audit (IA)

- **Definition:** IA is the organizational unit within the bank that is designated to fulfill the role and responsibilities with respect to the bank's internal audit system under the OCC's regulations.
- **Independence:** IA maintains independence from FLUs and IRM through the following reporting structure:
  - The board's audit committee reviews and approves IA's overall charter, risk assessments, and audit plans.
  - The board's audit committee approves all decisions regarding the appointment or removal of the CAE (the head of IA) and approves the annual compensation and salary adjustment of the CAE.
  - The CEO oversees the CAE's day-to-day activities.\*
  - No FLU executive oversees IA.
- **Accountability:** IA should be held accountable by the CEO and the board of directors for compliance with the risk governance guidelines. See [page 43](#) (IA responsibilities).

\* At some banks, the board's audit committee may assume the CEO's responsibilities for overseeing the CAE's day-to-day activities. This is an acceptable governance structure under the OCC's risk governance guidelines.

# Front Line Unit Responsibilities – Checklist

FLUs should take responsibility and be held accountable by the CEO and the board of directors for appropriately assessing and effectively managing all of the risks associated with their activities. Specifically, **each** FLU should:

- Assess, on an ongoing basis, the material risks associated with the FLU's activities and use such risk assessments as the basis for fulfilling its responsibilities under the guidelines and for determining if actions need to be taken to strengthen risk management or reduce risk given changes in the FLU's risk profile or other conditions.
  - E.g.*, there may be instances where an FLU should take action to manage risk effectively, even if the bank's risk appetite or applicable concentration risk limits, or the FLU's risk limits have not been exceeded.
- Establish and adhere to a set of written policies that include FLU risk limits. See [page 57](#).
  - Such policies should be based on ongoing risk assessments and should ensure that risks associated with the FLU's activities are effectively identified, measured, monitored and controlled, consistent with the bank's risk appetite statement, concentration risk limits and all policies established under the risk governance framework.

## Front Line Unit Responsibilities – Checklist *(cont.)*

- Establish and adhere to procedures and processes, as necessary based on ongoing risk assessments, to ensure compliance with the aforementioned written policies.
  - E.g.*, an FLU's processes for establishing its policies should provide for IRM's review and approval of these policies to ensure they are consistent with other policies established under the risk governance framework.
- Adhere to all applicable policies, procedures and processes established by IRM.
- Monitor compliance with applicable risk limits and report to IRM at least quarterly.
- Identify breaches of the risk appetite statement, concentration risk limits and FLU risk limits. Establish protocols for when and how to inform the board of directors, FLU management, IRM and the OCC of a risk limit breach that takes into account the severity of the breach and its impact on the bank. See [page 60](#) (processes governing risk limit breaches)
- Incorporate the bank's risk appetite statement, concentration risk limits and FLU risk limits into other decisions, plans, processes and programs. See [page 63](#) (relationship of risk appetite statement, concentration limits and FLU risk limits to other processes).

## Front Line Unit Responsibilities – Checklist *(cont.)*

- Ensure that the board of directors has sufficient information regarding the bank’s risk profile and risk management practices to provide credible challenges to management’s recommendations and decisions.
- Develop, attract and retain talent and maintain staffing levels required to carry out the FLU’s responsibilities effectively.
- Establish and adhere to talent management processes that comply with the guidelines. See [page 66](#).
- Establish and adhere to performance management and compensation programs that comply with the guidelines. See [page 67](#).

# Independent Risk Management Responsibilities – Checklist

IRM should oversee the bank's risk-taking activities and assess risks and issues independent of the CEO and FLUs. IRM should be held accountable by the CEO and the board of directors for fulfilling its responsibilities under the risk governance guidelines. Specifically, IRM should:

- Take primary responsibility for designing a comprehensive written risk governance framework that meets the risk governance guidelines and is commensurate with the size, complexity and risk profile of the bank. See [page 48](#) (written risk governance framework).
- Identify and assess, on an ongoing basis, the bank's material aggregate risks and use such risk assessments as the basis for fulfilling IRM's responsibilities 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.
  - E.g.*, there may be instances where IRM should take action to effectively manage risk, even if the bank's risk appetite or applicable concentration risk limits, or an FLU's risk limits have not been exceeded.

# Independent Risk Management Responsibilities – Checklist *(cont.)*

- Ensure that FLUs carry out their responsibilities under the risk governance guidelines.
- Establish and adhere to enterprise policies that include concentration risk limits. See [page 57](#).
  - 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 under the risk governance framework.
- Establish and adhere to procedures and processes, as necessary to ensure compliance with required enterprise policies.
- Identify and communicate to the CEO and the board of directors or the board’s risk committee:
  - Material risks and significant instances where IRM’s assessment of risk differs from that of an FLU; and
  - Significant instances where an FLU is not adhering to the risk governance framework.

# Independent Risk Management Responsibilities – Checklist *(cont.)*

- Identify and communicate to the board of directors or the board’s risk committee:
  - Material risks and significant instances where IRM’s assessment of risk differs from the CEO; and
  - Significant instances where the CEO is not adhering to, or holding FLUs accountable for adhering to, the risk governance framework.
- Monitor the bank’s risk profile in relation to its risk appetite and compliance with concentration risk limits and report such monitoring to the board of directors at least quarterly.
- When necessary due to the level and type of risk, monitor FLUs’ compliance with FLU risk limits and engage in ongoing communication with FLUs regarding adherence to these limits.
- Identify breaches of the risk appetite statement, concentration risk limits and FLU risk limits. Establish protocols for when and how to inform the board of directors, FLU management, IRM and the OCC of a risk limit breach that takes into account the severity of the breach and its impact on the bank. See [page 59](#) (risk appetite monitoring and communication processes).

# Independent Risk Management Responsibilities – Checklist *(cont.)*

- Incorporate the bank's risk appetite statement, concentration risk limits and FLU risk limits into other decisions, plans, processes and programs. See [page 63](#) (relationship of risk appetite statement, concentration limits and FLU risk limits to other processes).
- Ensure that the board of directors has sufficient information regarding the bank's risk profile and risk management practices to provide credible challenges to management's recommendations and decisions.
- Develop, attract and retain talent and maintain staffing levels required to carry out IRM's responsibilities effectively.
- Establish and adhere to talent management processes that comply with the guidelines. See [page 66](#).
- Establish and adhere to performance management and compensation programs that comply with the guidelines. See [page 67](#).

# Internal Audit Responsibilities – Checklist

In addition to meeting the standards set forth in the OCC's existing regulations,<sup>\*</sup> IA should ensure that the bank's risk governance framework complies with the OCC's risk governance guidelines and is appropriate for the size, complexity and risk profile of the bank. Specifically, IA 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.
- 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. See [page 64](#) (audit plan).
  - The audit plan should require IA to evaluate the adequacy of and compliance with policies, procedures and processes established by FLUs and IRM under the risk governance framework.
  - Changes to the audit plan should be communicated to the board's audit committee.

## Internal Audit Responsibilities – Checklist *(cont.)*

- Report in writing, conclusions, issues and recommendations from audit work carried out under the audit plan to the board's audit committee. IA's reports to the audit committee 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;
    - A determination of the effectiveness of FLUs and IRM in identifying and resolving issues in a timely manner;
  - Address potential and emerging concerns, the timeliness of corrective actions and the status of outstanding issues;
  - Include objective measures that enable the identification, measurement and monitoring of risk and internal control issues; and
  - Comment on the effectiveness of FLUs 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 Responsibilities – Checklist *(cont.)*

- Establish and adhere to processes for independently assessing the design and effectiveness of the risk governance 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 the risk governance guidelines and the degree to which the bank's risk governance framework is consistent with leading industry practices.
  - The annual independent assessment of the risk governance framework may be conducted by IA, an external party or IA in conjunction with an external party.
- Identify and communicate to the board's audit committee significant instances where FLUs or IRM are not adhering to the risk governance framework.
- Establish a quality assurance department that ensures IA'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 Responsibilities – Checklist *(cont.)*

- Ensure that the board of directors has sufficient information regarding the bank’s risk profile and risk management practices to provide credible challenges to management’s recommendations and decisions.
- Develop, attract and retain talent and maintain staffing levels required to carry out IA’s responsibilities effectively.
- Establish and adhere to talent management processes that comply with the guidelines. See [page 66](#).
- Establish and adhere to performance management and compensation programs that comply with the guidelines. See [page 67](#).

### **III. Risk Governance Framework:** Policies, Procedures, Processes and Programs

# Written Risk Governance Framework

- A bank must establish and adhere to a formal, written risk governance framework that is designed by IRM and approved by the board of directors or the board's risk committee.

Board / Risk Comm. CEO CRE IRM

- **Updates:** IRM 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.

Board / Risk Comm. CEO CRE IRM

- **Roles and Responsibilities:** The board of directors, senior management and each of the three lines of defense have separate roles and responsibilities under the risk governance framework. See [page 21](#) (board of directors responsibilities), [page 29](#) (senior management responsibilities) and [page 36](#) (three lines of defense responsibilities).

Board Risk Comm. Audit Comm. CEO CRE CAE FLUs IRM IA

# Written Risk Governance Framework *(cont.)*

- **Scope of Risks Covered:** The written 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
  - Reputation risk
- The OCC has defined these eight categories of risks for supervision purposes, but a bank may choose to categorize underlying risks in a different manner for risk management purposes.
- Regardless of how a bank categorizes its risks, the risk governance 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.

# Written Strategic Plan

- The bank's CEO should develop a written strategic plan with input from the three lines of defense. **CEO** **CRE** **CAE** **FLUs** **IRM** **IA**
- The board of directors should evaluate and approve the strategic plan and monitor management's efforts to implement the strategic plan at least annually. **Board**
- **Contents of Strategic Plan:** The strategic plan should:
  - Cover, at a minimum, a three-year period;
  - Contain a comprehensive assessment of risks that currently impact the bank or could impact the bank during the period covered by the plan;
  - Articulate overall mission statement and strategic objectives for the bank and how it will achieve those objectives;
  - Include an explanation of how the bank will update, as necessary, the risk governance framework to account for changes in its risk profile projected under the plan; and
  - 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 plan was developed.

# A Bank's Risk Profile

- The OCC's risk governance guidelines include numerous references to a bank's risk profile.
- **Definition:** Risk profile is a point-in-time assessment of a bank's risks, aggregated within and across each relevant risk category (*i.e.*, credit risk, interest rate risk, liquidity risk, price risk, operational risk, compliance risk, strategic risk and reputational risk), using methodologies consistent with the bank's written risk appetite statement.
- **Preparation of Risk Profile:** IRM should prepare an assessment of the bank's risks with input from FLUs. **FLUs** **IRM**
- **Review:** The CEO, in conjunction with the board of directors or the board's risk committee, should ensure that IRM's assessment is comprehensive, understand the assumptions used by IRM 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. **Board** / **Risk Comm.** **CEO**
- **Independent Assessment:** IA should provide an independent assessment of the comprehensiveness of IRM's assessment and challenge assumptions that it deems to be inappropriate. **IA**
- **OCC Examiners:** As part of their supervisory activities, OCC examiners will assess the integrity of the process used to prepare the assessment and communicate any concerns regarding the process or IRM's depiction of the bank's risk profile to the CEO and board of directors. **OCC** **Board** **CEO**

# Written Risk Appetite Statement

- A bank should have a comprehensive written statement that articulates the bank's risk appetite and serves as the basis for the risk governance framework.
  - **Risk appetite** is the aggregate level and type 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.
- **Board Review and Approval:** The risk appetite statement should be reviewed and approved 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. **Board** / **Risk Comm.**

# Written Risk Appetite Statement: Contents

- The risk appetite statement should include both qualitative components and quantitative limits.
- **Qualitative components** describe a safe and sound risk culture and how the bank will assess and accept risks, including those that are difficult to quantify. See [page 54](#) (safe and sound risk culture).
- **Quantitative limits** should:
  - Incorporate sound stress testing processes, as appropriate;
  - Address bank 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 earnings, liquidity and capital.\* See [page 55](#) (setting quantitative limits).

\* Where possible, a bank should establish aggregate risk appetite limits that can be disaggregated and applied at the FLU level. However, where this is not possible, a bank should establish limits that reasonably reflect the aggregate level of risk that the board of directors and senior management are willing to accept.

# Written Risk Appetite Statement: Safe and Sound Risk Culture

- A bank's risk appetite statement should describe the bank's safe and sound risk culture.
- Risk culture refers to shared values, attitudes, competencies and behaviors present throughout the bank that shape and influence governance practices and risk decisions.
- Setting an appropriate tone at the top is critical to establishing a sound risk culture, and the risk appetite statement should articulate the core values that the board and CEO expect bank employees to share when carrying out their respective roles and responsibilities.
- 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, board committees, senior management and other individuals.
- Evidence of a sound risk culture includes, but is not limited to:
  - Open dialogue and transparent sharing of information among FLUs, IRM and IA;
  - Consideration of all relevant risks and the views of IRM and IA in risk-taking decisions; and
  - Compensation and performance management programs and decisions that reward compliance with the core values and quantitative limits established in the risk appetite statement; and
  - Holding accountable those who do not conduct themselves in a manner consistent with the standards articulated in the risk appetite statement.

# Written Risk Appetite Statement: Setting Quantitative Limits

- A bank may set quantitative limits on a gross or net basis that take into account appropriate capital and liquidity buffers.
- Risk limits may be designed as thresholds, triggers or hard limits, depending on how the board of directors and management choose to manage risk.
  - Thresholds or triggers that prompt discussion and action before a hard limit is reached or breached can be useful tools for reinforcing risk appetite and proactively responding to elevated risk indicators.
- Limits should be set at levels that prompt the board and management 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. Accordingly, these indicators are generally not useful in proactively managing risk.

# Written Risk Appetite Statement: Setting Quantitative Limits *(cont.)*

- Setting quantitative limits based on performance under various **stress scenarios** may enable the board and management to take actions that reduce risk before delinquencies, problem assets and losses reach excessive levels.
  - OCC examiners will apply judgment when determining which quantitative limits should be based on stress testing. They will consider several factors, including: **OCC**
    - The value in using such measures for the risk type;
    - The bank's ability to produce such measures;
    - The capabilities of similarly-situated banks; and
    - The degree to which the bank's board and management have invested in the resources needed to establish such capabilities.
  - The U.S. banking agencies' May 2012 stress testing guidance describes various stress testing approaches and applications.
    - A bank should consider the range of approaches and select the one(s) most suitable when establishing quantitative limits.

# Concentration and Front Line Unit Risk Limits

- A bank's risk governance framework should include for the relevant risk categories:
  - **Concentration risk limits**;<sup>\*</sup> and
  - As applicable, **FLU risk limits**.
- The relevant risks include:
  - Credit risk
  - Interest rate risk
  - Liquidity risk
  - Price risk
  - Operational risk
  - Compliance risk
  - Strategic risk
  - Reputation risk
- Concentration and front line unit risk limits should ensure that FLUs 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.
  - Depending on a bank's organizational structure, concentration risk limits and FLU risk limits may also need to be established for legal entities, units based on geographical areas or product lines.

<sup>\*</sup> 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 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.

# Concentration Risk Management

- A bank's 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.
- Concentrations of risk can arise in any risk category, with the most common being identified with borrowers, fund providers and counterparties. Concentrations can exist both on and off the balance sheet.
- The OCC's eight categories of risk (credit risk, interest rate risk, liquidity risk, price risk, operational risk, compliance risk, strategic risk and reputational risk) are not mutually exclusive.
  - Any product or service may expose a bank to multiple risks, and risks may also be interdependent.
- The OCC expects a bank to continually enhance its concentration risk management processes to strengthen its ability to effectively identify, measure, monitor and control concentrations that arise in all risk categories.

# Risk Appetite Monitoring and Communication Processes

A bank's risk governance framework should provide for:

- 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.
- Monitoring by IRM 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. **Board** / **Risk Comm.** **CRE** **IRM**
- Monitoring by FLUs of compliance with their respective risk limits and reporting to IRM at least quarterly. **CRE** **FLUs** **IRM**
- When necessary due to the level and type of risk:
  - Monitoring by IRM of FLUs' compliance with FLU risk limits;
  - Ongoing communication with FLUs regarding adherence to these limits; and
  - Reporting of any concerns to the CEO and the board of directors or the board's risk committee. **Board** / **Risk Comm.** **CEO** **CRE** **FLUs** **IRM**

# Processes Governing Risk Limit Breaches

The bank should establish and adhere to processes that require FLUs and IRM, in conjunction with their respective responsibilities, to:

- Identify breaches of the risk appetite statement, concentration risk limits and FLU risk limits. **CEO** **CRE** **FLUs** **IRM**
- Distinguish breaches based on the severity of their impact on the bank.
- Establish protocols for when and how to inform the board of directors, FLU management, IRM and the OCC of a risk limit breach that takes into account the severity of the breach and its impact on the bank. **Board** **Risk Comm.** **CEO** **CRE** **FLUs** **IRM**
  - Risk limit breach protocols should include a written description of how a breach will be, or has been resolved.
- 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. **CEO** **CRE** **FLUs** **IRM**
- A bank may have different escalation and resolution processes for breaches of its risk appetite statement, concentration risk limits and FLU risk limits.

# Risk Data Aggregation and Reporting

- The OCC expects a bank 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.
- A bank's 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.
- These policies, procedures and processes should provide for:
  - 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;
  - 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
  - The distribution of risk reports to all relevant parties at a frequency that meets their needs for decision-making purposes.

# Risk Data Aggregation and Reporting: OCC's Expectations for G-SIBs

- In January 2013, the Basel Committee on Banking Supervision (Basel Committee) 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 bank subsidiaries of G-SIBs that it supervises to be largely compliant with the Basel Committee's principles by the beginning of 2016.
- Banks that are not subsidiaries of G-SIBs are **not** expected to comply with the Basel Committee's principles by the beginning of 2016.
  - However, the OCC stated that these banks should consider the Basel Committee's principles to be leading practices and should make an effort to bring their practices into alignment with the principles where possible.

# Relationship of Risk Appetite Statement, Concentration Limits and FLU Risk Limits to Other Processes

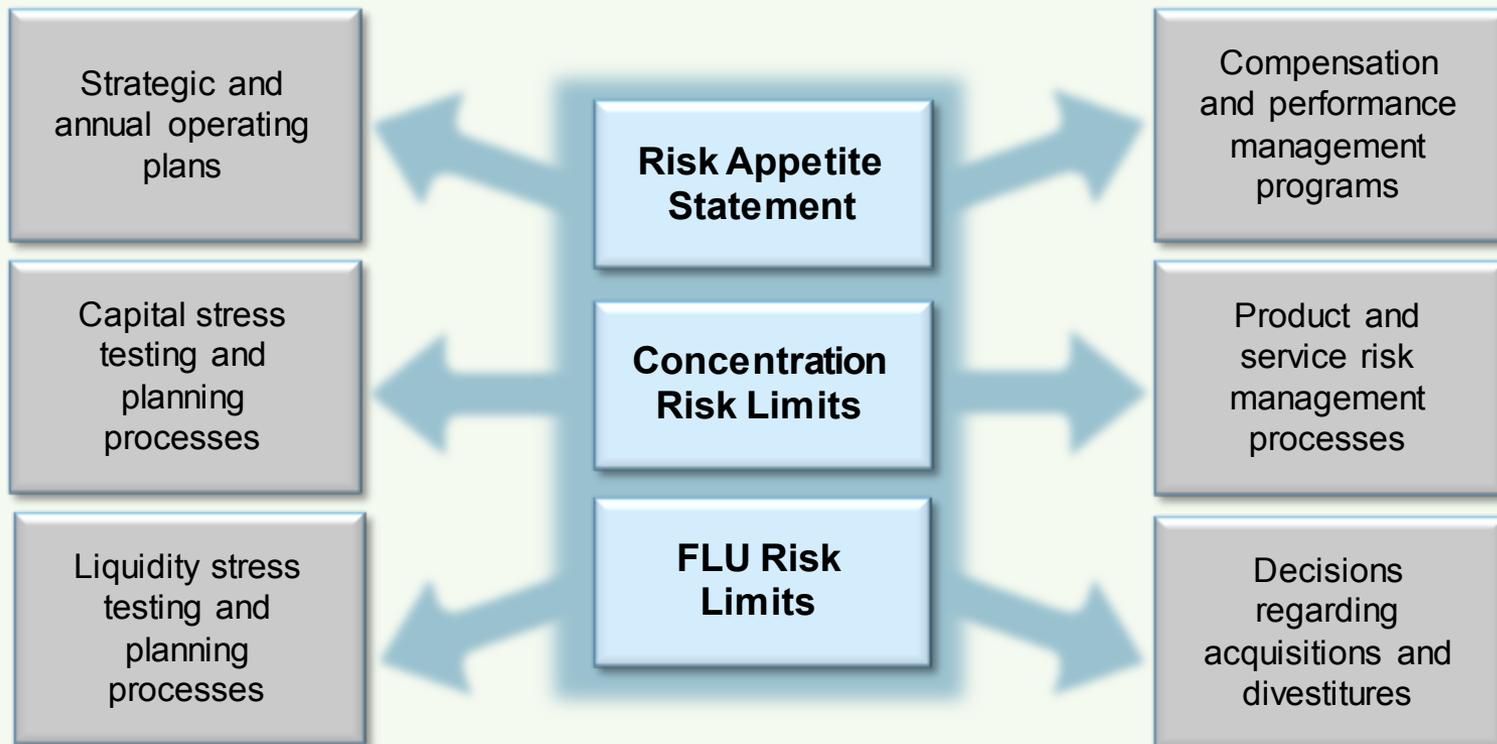
- A bank's FLUs and IRM should incorporate the risk appetite statement, concentration risk limits and FLU risk limits into other decisions, plans, processes and programs:

CEO

CRE

FLUs

IRM



# Audit Plan

- IA is responsible for designing and implementing an audit plan that is reviewed by the board's audit committee. Audit Comm. CAE IA
- IA should maintain a complete and current inventory of all of the bank's material businesses, product lines, services and functions that serve as the basis for the audit plan.
- **Contents of the Audit Plan:** The audit plan should:
  - Rate the risks presented by each FLU, product line, service and function, including activities that the bank may outsource to a third party.
    - IA should derive these ratings from its bank-wide risk assessments and should periodically adjust these ratings based on risk assessments conducted by FLUs and changes in the bank's strategy and the external environment.
  - Include ongoing monitoring to identify emerging risks and ensure that units, product lines, services and functions that receive a low risk rating are reevaluated with reasonable frequency.
  - Take into account the bank's risk profile as well as emerging risks and issues.

# Audit Plan *(cont.)*

- **Contents of the Audit Plan *(cont.)*:**

- Require IA to evaluate adequacy of and compliance with policies, procedures and processes established by FLUs and IRM under the risk governance framework.
  - This evaluation is in addition to IA'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.
  - The audit plan should require the evaluation of reputation and strategic risk, along with evaluations of IRM and traditional risks.

- **Updates to the Audit Plan**

- The audit plan should be updated at least quarterly or more often as needed.
- All changes to the audit plan should be communicated to the board's audit committee.

Audit Comm.

CAE

IA

# Talent Management Processes

- A 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.
- A bank's talent management process should ensure that the board of directors or a committee thereof: **Board** / **Board Comm.**
  - Hires a CEO and approves the hiring of direct reports of the CEO, including the CRE and CAE, with the skills and abilities to design and implement an effective risk governance framework.
  - Establishes reliable succession plans for the CEO and his or her direct reports, including the CRE and CAE.
  - Oversees the talent development, recruitment and succession planning processes for individuals two levels down from the CEO.
  - Oversees the talent development, recruitment and succession planning processes for IRM and IA.

# Compensation and Performance Management Programs

A bank should establish and adhere to compensation and performance management programs to meet the requirements of any applicable statute or regulation and that are appropriate to: **Board** / **Board Comm.** **CEO** **CRE** **CAE**

- Ensure that the CEO, FLUs, IRM and IA implement and adhere to an effective risk governance framework.
- Ensure that FLU compensation plans and decisions appropriately consider the level and severity of issues and concerns identified by IRM and IA.
- Attract and retain the talent needed to design, implement and maintain an effective risk governance framework.
- 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.

## **IV. Risk Governance Framework:**

Relationship Between Subsidiary Bank's and Parent Company's Risk Governance Frameworks

# A Bank Must Generally Develop Its Own Risk Governance Framework

- Generally, a bank must develop its own risk governance framework.
- **Limited Exception:** A bank may use its parent company's risk governance framework to satisfy the OCC's risk governance guidelines if **all** of the following requirements are satisfied:
  - The bank's risk profile is substantially the same as its parent company's risk profile, meaning:
    - As of the most recent quarter-end call report, the bank's average total consolidated assets, total assets under management and total off-balance sheet exposures each represent  $\geq 95\%$  of the parent company's; or
    - The bank demonstrates to the OCC that the risk profiles of the parent company and the bank are substantially the same based on other factors.
  - **The parent company's risk governance framework complies with the OCC's risk governance 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.

# Using Components of Parent Company's Risk Governance Framework

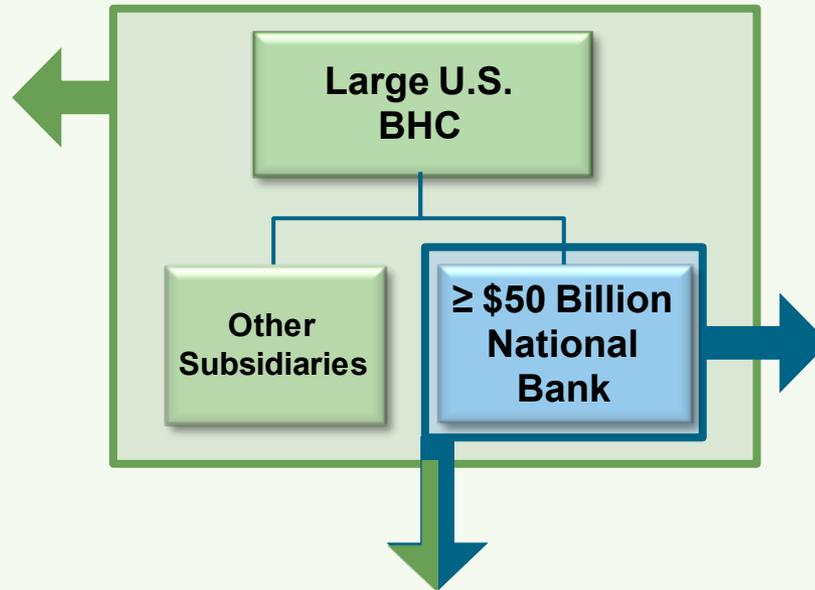
- A bank may use **certain components** of the parent company's risk governance framework even if the bank's risk profile is not substantially the same as its parent's risk profile.
- However, the bank's risk governance framework should ensure that:
  - The bank's risk profile is easily distinguished and separate from the parent company's risk profile for risk management and supervisory reporting purposes; and
  - 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 a bank in determining which components of a parent company's risk governance framework may be used. **OCC**

# OCC Guidelines and Dodd-Frank Enhanced Risk Management Standards for Large U.S. BHCs

## Federal Reserve's Dodd-Frank Section 165 Proposal

Requires a U.S. BHC with  $\geq$  \$50 billion in total consolidated assets to comply with the following enhanced risk management standards:

- Must establish an enterprise-wide risk committee within the top-tier holding company's board of directors.
- Risk committee must document, review and approve the BHC's enterprise-wide risk management practices.
- Must appoint a chief risk officer with specified enterprise-wide risk management responsibilities.



## OCC's Risk Governance Guidelines

Sets new, and much higher, minimum standards for:

- The design and implementation of a bank's own risk governance framework; and
- The oversight by the bank's board of directors of the bank's risk governance framework.

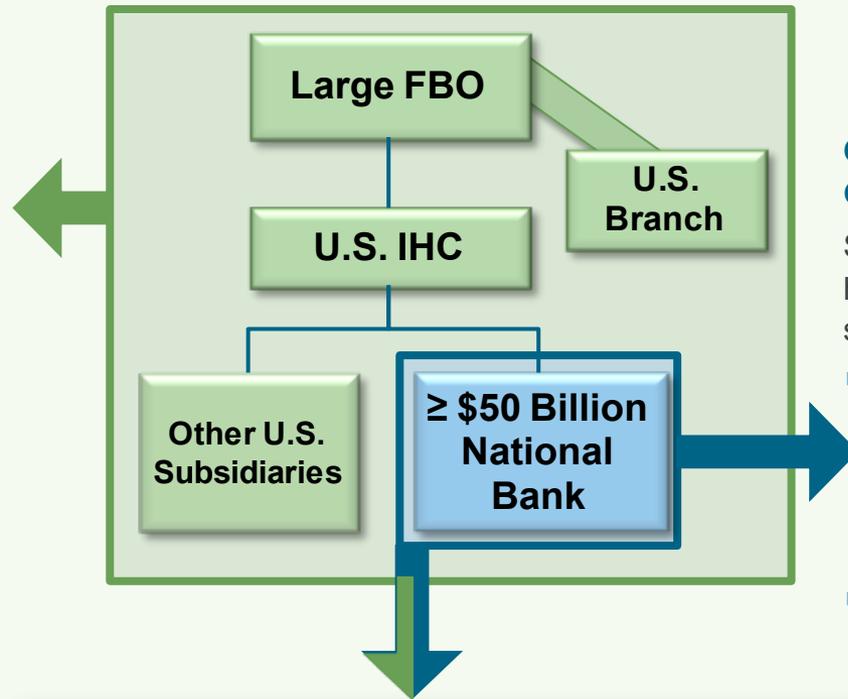
**Integration:** The BHC's Dodd-Frank enhanced risk management program should be integrated with its subsidiary bank's risk governance framework

# OCC Guidelines and Dodd-Frank Enhanced Risk Management Standards for Large FBOs

## Federal Reserve's Dodd-Frank Section 165 Proposal

Requires an FBO with  $\geq$  \$50 billion in combined U.S. assets to comply with the following enhanced risk management standards:

- Must establish a U.S. risk committee within the board of directors of either the FBO or the U.S. intermediate holding company (IHC).
- U.S. risk committee must oversee the risk management practices of the FBO's U.S. subsidiaries and U.S. branches and agencies (combined U.S. operations).
- Must appoint a U.S. chief risk officer with specified risk management responsibilities for the combined U.S. operations.



## OCC's Risk Governance Guidelines

Sets new, and much higher, minimum standards for:

- The design and implementation of a bank's own risk governance framework; and
- The oversight by the bank's board of directors of the bank's risk governance framework.

**Integration:** The large FBO's Dodd-Frank enhanced risk management program should be integrated with its subsidiary bank's risk governance framework

# Davis Polk Contacts

If you have any questions regarding the matters covered in this publication, please contact any of the lawyers listed below or your regular Davis Polk contact.

<b>Luigi L. De Ghenghi</b>	212 450 4296	<a href="mailto:luigi.deghenghi@davispolk.com">luigi.deghenghi@davispolk.com</a>
<b>Randall D. Guynn</b>	212 450 4239	<a href="mailto:randall.guynn@davispolk.com">randall.guynn@davispolk.com</a>
<b>Lena V. Kiely</b>	212 450 4619	<a href="mailto:lena.kiely@davispolk.com">lena.kiely@davispolk.com</a>
<b>Reena Agrawal Sahni</b>	212 450 4801	<a href="mailto:reena.sahni@davispolk.com">reena.sahni@davispolk.com</a>
<b>Margaret E. Tahyar</b>	212 450 4379	<a href="mailto:margaret.tahyar@davispolk.com">margaret.tahyar@davispolk.com</a>
<b>Andrew S. Fei</b>	212 450 4063	<a href="mailto:andrew.feii@davispolk.com">andrew.feii@davispolk.com</a>