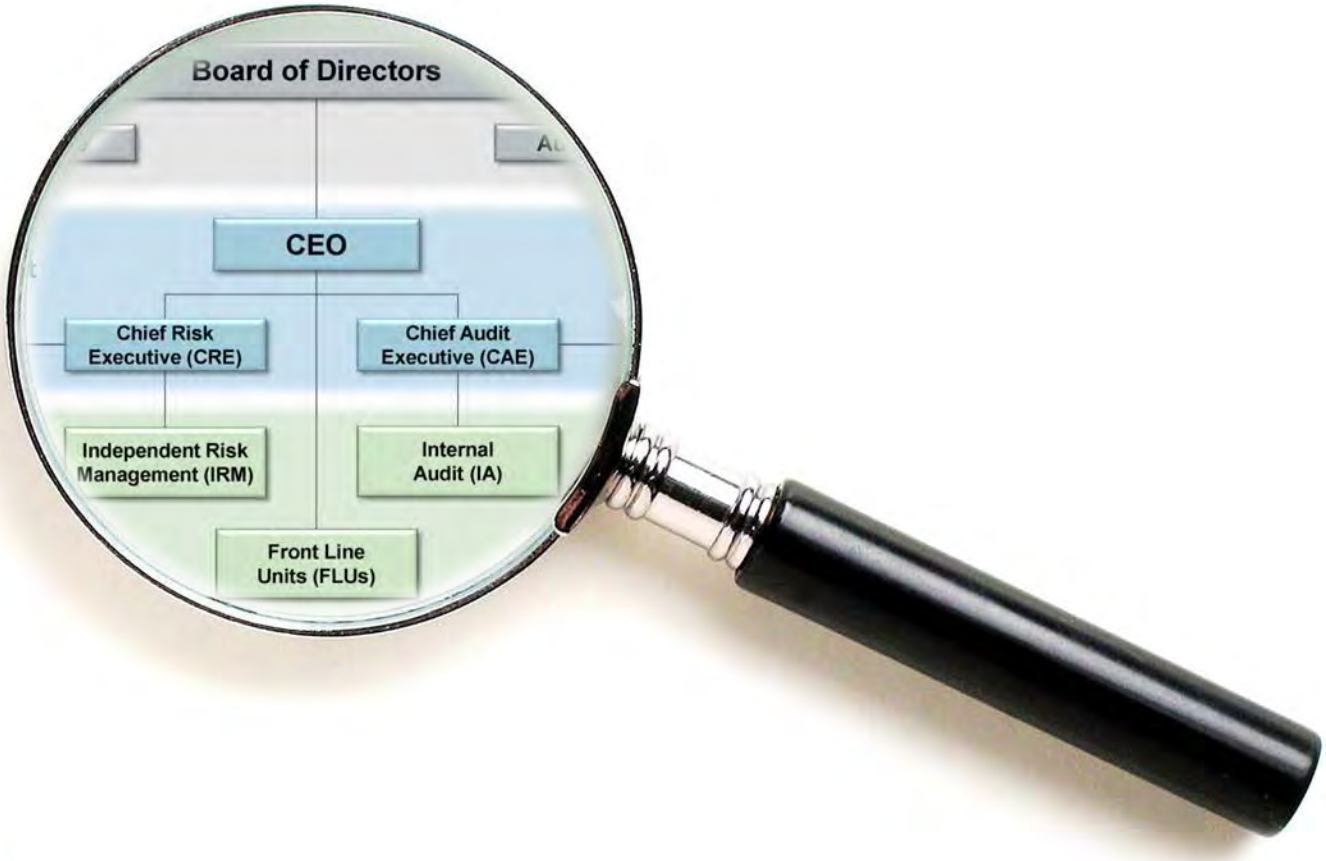
Risk Governance

Visual Memorandum on Guidelines Adopted by the OCC



November 7, 2014

Davis Polk

Davis Polk & Wardwell LLP

Table of Contents

Click on an item to go to that page

Davis Polk

Table of Contents *(cont.)*

Click on an item to go to that page

Davis Polk

Table of Contents *(cont.)*

Click on an item to go to that page

Davis Polk

Table of Contents *(cont.)*

Click on an item to go to that page

Davis Polk

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

Davis Polk

Overview of the OCC's Risk Governance Guidelines

- After the financial crisis, the OCC 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 9**.
- January 2014: the OCC proposed a set of **enforceable** and specific **risk governance guidelines** to formalize those heightened expectations for **insured** national banks, federal savings associations and federal branches of foreign banks with **≥ $50 billion** in average total consolidated assets.
- September 2, 2014: the OCC adopted final risk governance guidelines.
  - The final guidelines also apply to a bank with < $50 billion in average total consolidated assets if its parent company controls at least one ≥ $50 billion bank.
- The risk governance guidelines establish new 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 are not subject to the OCC's risk governance guidelines, but similar principles likely will be applied by the Federal Reserve and the FDIC to large state member and non-member banks.

Davis Polk

Overview of the OCC's Risk Governance Guidelines *(cont.)*

- **Mid-size Banks:** OCC may apply the risk governance guidelines to a < $50 billion bank not under common control with a ≥ $50 billion bank if it determines that the bank's operations are highly complex or otherwise present a heightened risk.
  - Comptroller said this reservation of authority will be used only in "extraordinary circumstances."
  - OCC does not intend to use reservation of authority to apply guidelines to community banks.

OCC's Heightened Expectations Program

- After the financial crisis, the OCC developed a set of **heightened expectations** to enhance its supervision and strengthen the risk management practices and governance of the largest national banks.
- The heightened expectations program focused on 5 risk governance requirements:
  - Preserving the sanctity of the bank charter
  - Maintaining a well-defined personnel management program
  - Defining and communicating an acceptable risk appetite
  - Maintaining reliable oversight programs
  - Board of directors providing a credible challenge to bank management's decision-making
- The OCC's new risk governance guidelines **supersede** the heightened expectations program.

Davis Polk

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).
- Other indications of this trend include the following:
  - In implementing the Dodd-Frank Act's enhanced prudential standards for large U.S. bank holding companies (BHCs), large foreign banking organizations (FBOs) and systemically important nonbank financial companies, the Federal Reserve has required large BHCs and FBOs to establish risk committees, appoint chief risk officers and satisfy other new risk management requirements.
  - Banking organizations are required to 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 rules and other legal and regulatory developments.

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

Davis Polk

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 22**.
- **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 24**.
- **Board of directors responsibilities** under the risk governance framework. *See* **page 25**.
- **Senior management responsibilities** under the risk governance framework. *See* **page 33**.
- **Responsibilities of the three lines of defense** that are fundamental to the design and implementation of the risk governance framework. *See* **page 42**.
- **Written risk governance framework and strategic plan**. *See* **page 54**.
- **Written risk appetite statement** that includes both qualitative components and quantitative limits and serves as a basis for the risk governance framework. *See* **page 58**.
- **Concentration and front line unit risk limits and processes**. *See* **page 63**.
- **Talent management processes, compensation and performance management programs** and other key aspects of the risk governance framework. *See* **page 72**.
- **Relationship between bank's and parent company's risk governance frameworks**. *See* **page 74**.
- **OCC's enforcement of the risk governance guidelines**. *See* **page 19**.
- **Compliance timeline**. *See* **page 18**.

Key Changes from Proposed Risk Governance Guidelines

- ***Using Parent Company Risk Governance Framework***
  - Simplified threshold for use of parent's framework by eliminating AUM and off-balance sheet exposure thresholds.
- ***Sister Banks and Other Bank Subsidiaries***
  - The final guidelines apply to any < $50 billion bank that is under common control with a ≥ $50 billion bank.
  - The OCC had declared that it would use its authority to apply the proposed guidelines to a "highly complex" < $50 billion bank in cases where a parent company owned two or more < $50 billion banks with combined assets ≥ $50 billion, but the OCC now states that it will use this authority only in extraordinary circumstances.
  - The OCC does **not** intend to use this authority to apply the guidelines to **community banks**.

Key Changes from Proposed Risk Governance Guidelines *(cont.)*

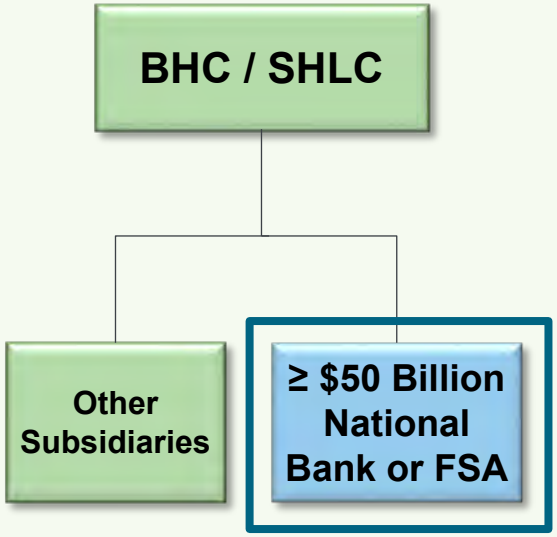
- ***Compliance Dates***
  - Staggered compliance dates from November 10, 2014 through May 10, 2016, depending on size of banks.
  - 18-month compliance deadline when a bank becomes a ≥ $50 billion bank.
- ***Board of Directors and Board Committees***
  - Clarified governance roles to be consistent with oversight rather than management responsibilities.
- ***Chief Executive Officer (CEO)***
  - Clarified responsibilities to eliminate oversight of "day-to-day activities" of Chief Risk Executive (CRE) and Chief Audit Executive (CAE).
- ***CRE***
  - Provided for more than one CRE and clarified aspects of the CRE's roles and responsibilities.

Key Changes from Proposed Risk Governance Guidelines *(cont.)*

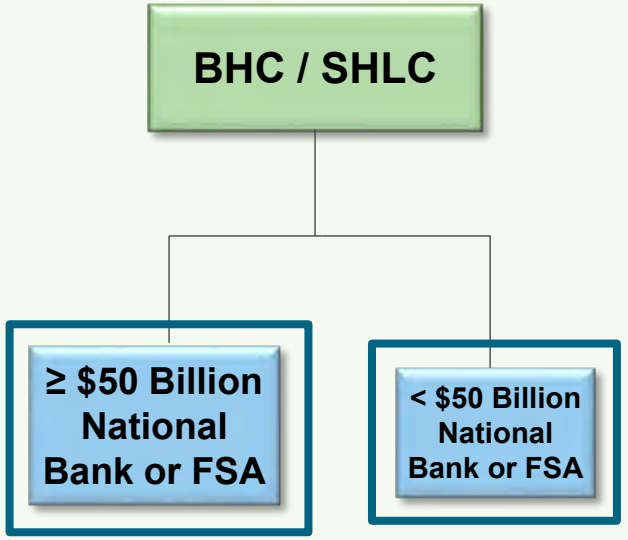
- ***Front Line Units (FLUs)***
  - Amended definition to include accountability of risk **and** other criteria, narrowing list of potential FLUs, and generally to exclude legal function.
- ***Independent Risk Management (IRM) and Internal Audit (IA)***
  - Clarified aspects of IRM's and IA's roles and responsibilities.

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

- The OCC's risk governance guidelines will apply to a broader group of banks than those that have been subject to the OCC's heightened expectations program.



The risk governance guidelines will apply to a ≥ $50 billion* insured national bank or federal savings association (FSA).



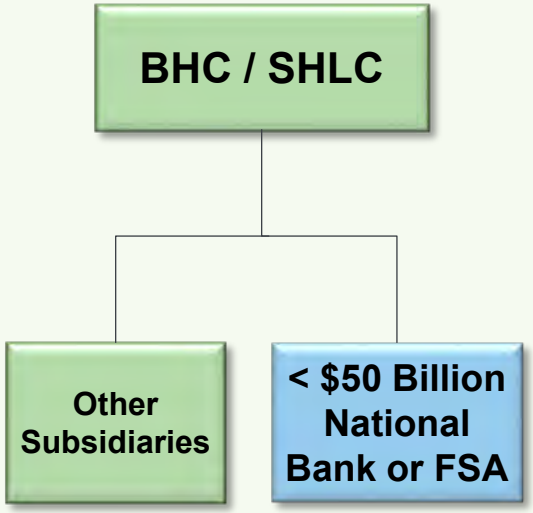
If a < $50 billion insured national bank or FSA is controlled by a parent company that also controls a ≥ $50 billion insured national bank or FSA, the risk guidelines will apply to that < $50 billion national bank or FSA.

* The asset threshold for the application of the risk governance guidelines is measured using a bank's average total consolidated assets for the four most recent consecutive quarters, as reported on the bank's call reports.

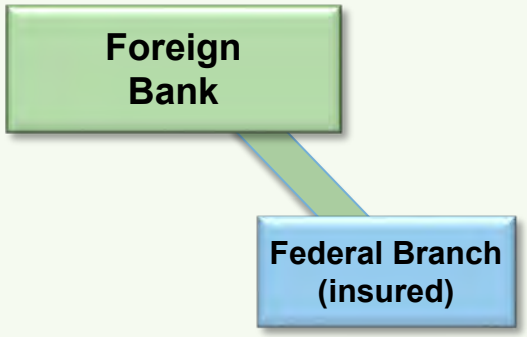
Davis Polk

Click here to return to table of contents

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



OCC Discretion: The OCC **may** apply the risk governance guidelines to a < $50 billion insured national bank or FSA if the OCC determines that the bank's operations are highly complex or otherwise present a heightened risk. The OCC notes that it intends to use this authority in **extraordinary circumstances**.



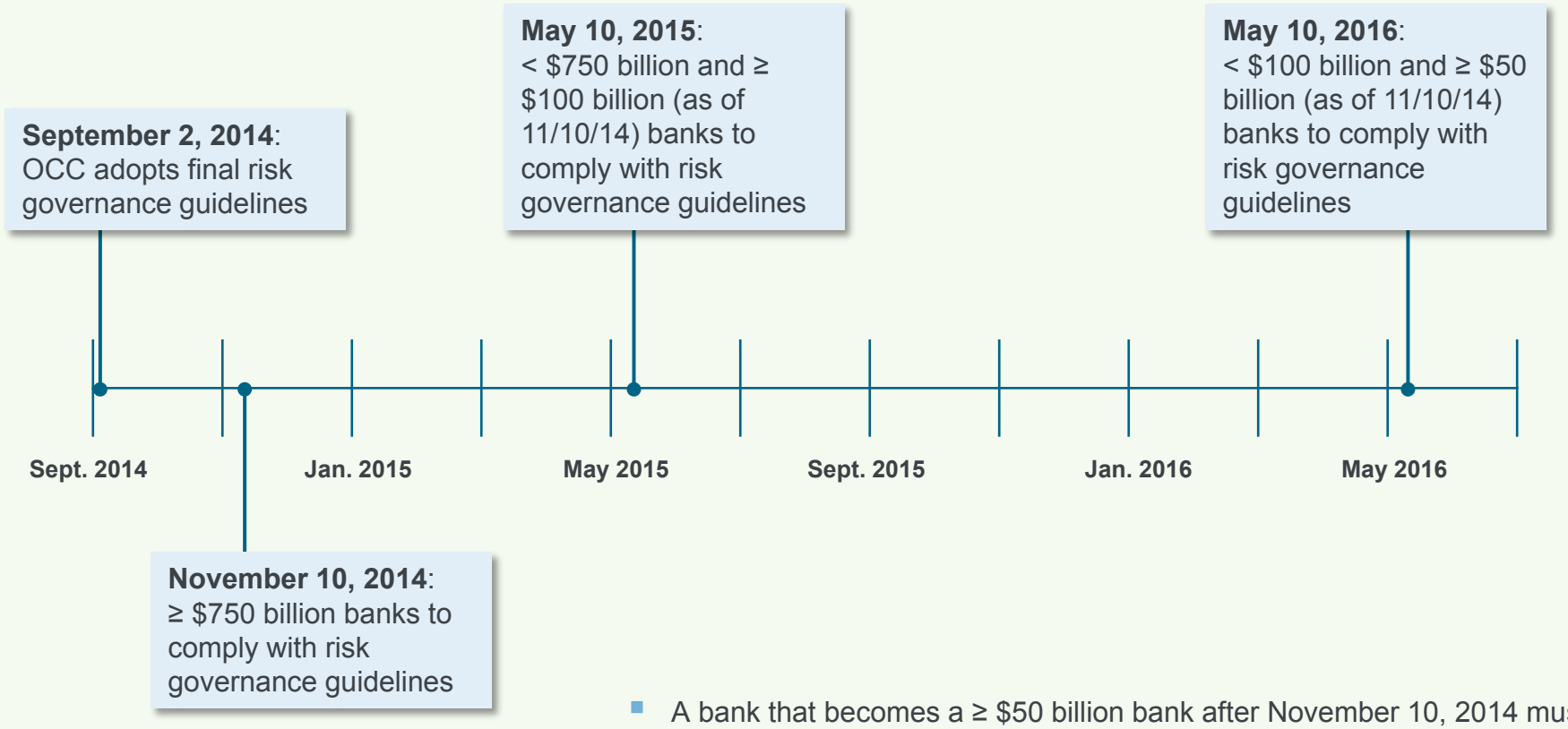
The OCC's risk governance guidelines will apply to a ≥ $50 billion **insured** federal branch of a foreign bank. Currently, no insured federal branch of a foreign bank is ≥ $50 billion.

A < $50 billion insured federal branch will be subject to the risk governance guidelines if it is under common control with a national bank, FSA or federal branch that is otherwise subject to the risk governance guidelines.

Davis Polk

Click here to return to table of contents

Compliance Dates for Risk Governance Guidelines



- A bank that becomes a ≥ $50 billion bank after November 10, 2014 must comply with the risk governance guidelines within 18 months of the as-of date of the call report showing the bank reaching at least $50 billion in average total assets for four consecutive quarters.

Davis Polk

Enforcement of the OCC's Risk Governance Guidelines

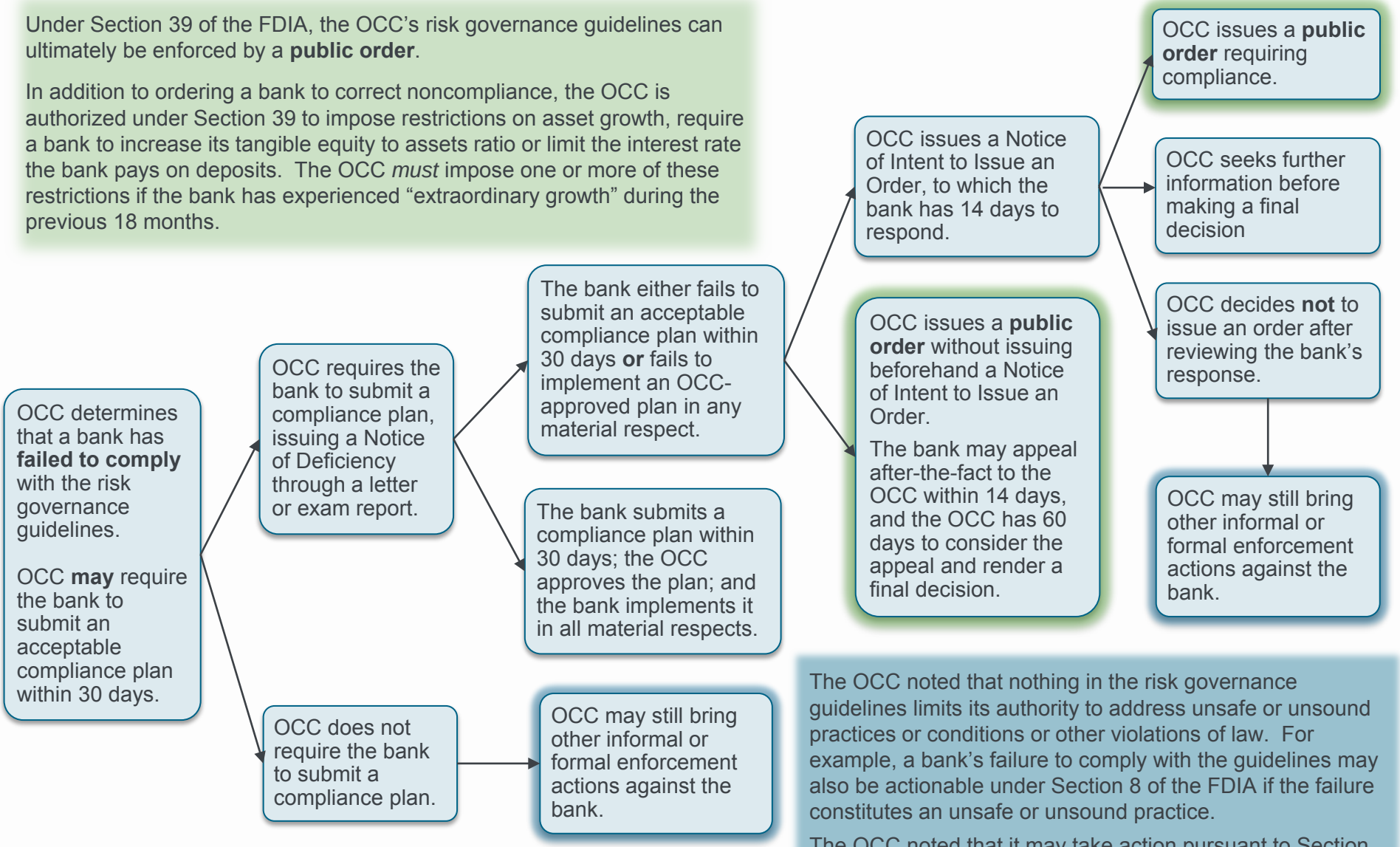
- **Enforcement is a key reason behind the formalization of the OCC's heightened expectations into specific guidelines.**
- The OCC adopted the risk governance guidelines pursuant to Section 39 of the Federal Deposit Insurance Act (FDIA).
- Section 39 authorizes the OCC to prescribe safety and soundness 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, the OCC **must** require the bank to submit a compliance plan specifying the steps it will take to comply with the 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 a regulation or a guideline ultimately may be enforced by an order.
  - Orders are formal, **public** actions 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 failure to comply and its self-corrective and remedial responses.

Section 39 Enforcement Procedures Flowchart

Davis Polk

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.

Click here to return to table of contents

II. Risk Governance Framework:

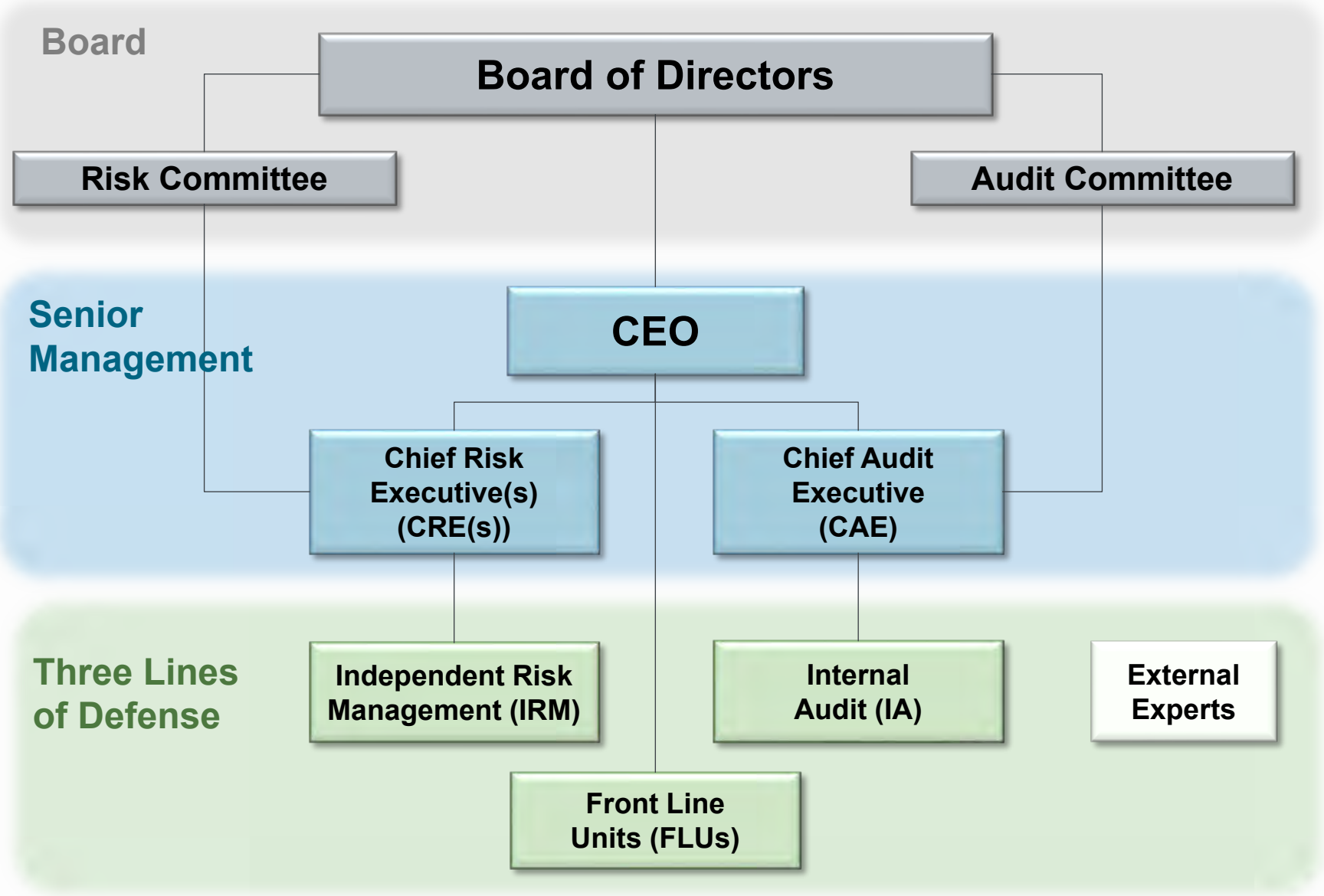
Structure and Responsibilities

Davis Polk

Risk Governance Structure

Davis Polk

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

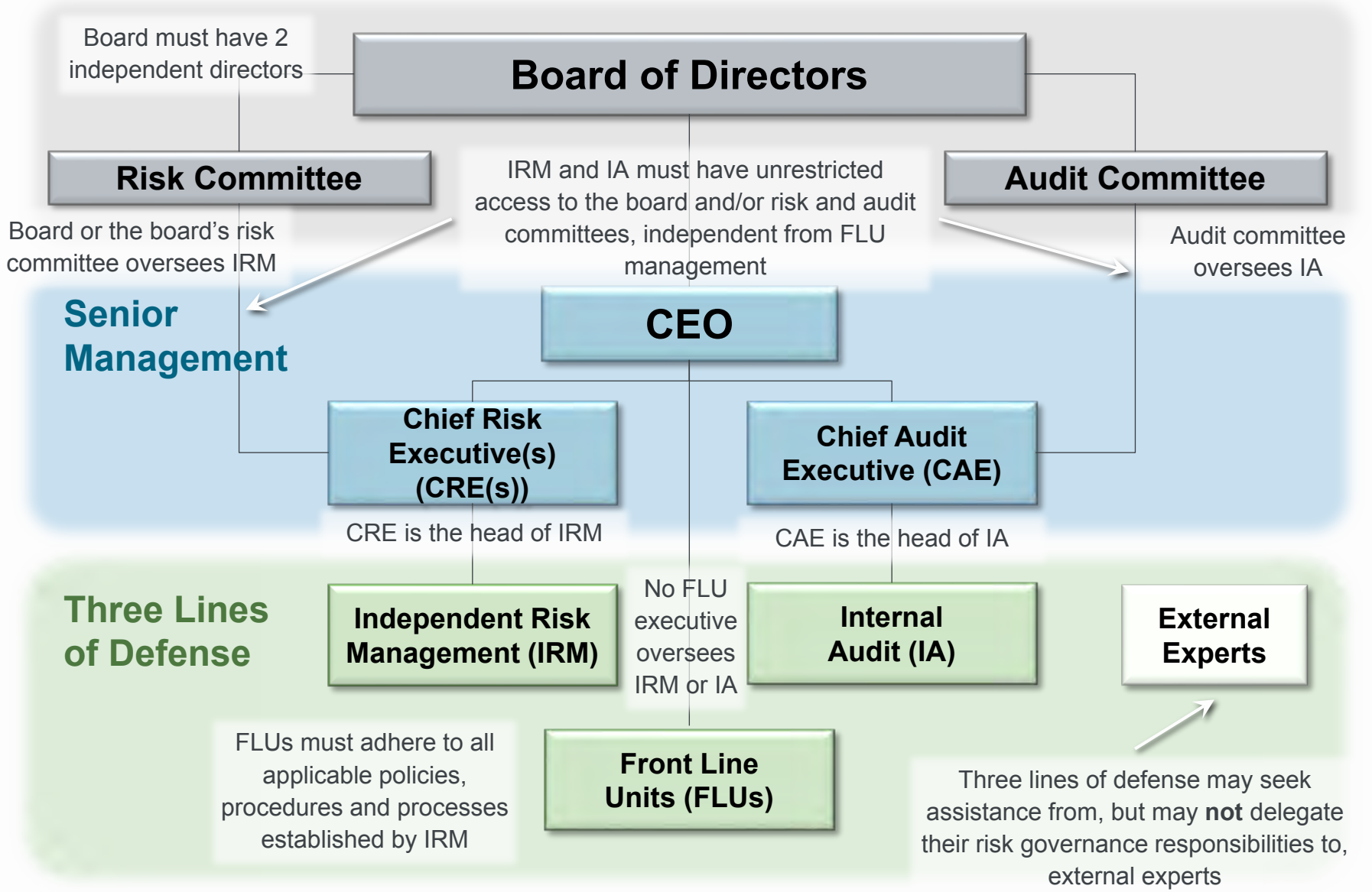


Click here to return to table of contents

Key Features of Risk Governance Structure

Davis Polk

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



Click here to return to table of contents

Board Composition Requirements:
Two Independent Directors

- The OCC's risk governance guidelines provide that a bank's board of directors should include at least **2 independent directors** who satisfy the same independence standard used in the Federal Reserve's enhanced prudential standards final rule under Section 165 of the Dodd-Frank Act.
  - These directors should:
    - Not be officers or employees of the bank or parent company, currently or during the previous 3 years
    - Not be members of the "immediate family" of a person who is, or has been within the last 3 years, an "executive officer" of the parent company or bank, as those terms are used in the Federal Reserve's Regulation Y and Regulation O, and
    - Qualify as independent under the listing standards of a national securities exchange.
- A number of large national banks already satisfy the 2 independent directors requirement.

Davis Polk

Board of Directors Responsibilities – Checklist

- **Require an Effective Risk Governance Framework:** Each member of the board of directors should oversee the bank's compliance with safe and sound banking practices. The board of directors should also require management to establish and implement an effective risk governance framework that meets the minimum standards 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 and any significant changes to the framework and monitor compliance with the framework. *See* **page 54**.
    - The final guidelines do not require the board or risk committee to review and approve any material policies established under the framework. The OCC clarified that these policies should be approved by management.
  - **Strategic Plan:** The board should evaluate and approve the strategic plan and monitor management's efforts to implement it at least annually. *See* **page 56**.
  - **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 58**.
  - **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 60**.

Davis Polk

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 may provide active oversight by relying on risk assessments and reports prepared by independent risk management and internal audit to 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 OCC clarified that the guidelines do not contemplate that the board would assume managerial responsibilities in overseeing management.
    - The board is permitted to rely on IRM and IA to meet these oversight responsibilities.
    - The OCC intends to assess compliance with this standard primarily through frequent examiner conversations with directors.
    - Board members should oppose management's recommendations only when necessary and are not expected to evidence opposition to management during each meeting.
    - The OCC notes that some boards may periodically engage third-party experts to assist them in understanding risks and issues and to make recommendations to strengthen board and bank practices.

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

- **Provide Active Oversight of Management** *(cont.)*
  - The board should hold FLUs accountable for, among other things, appropriately assessing and effectively managing all of the risks associated with the FLUs' activities.
    - *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.
  - 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.
- **Oversight of CRE(s) 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.
  - **Access by and Communications from CRE:** The CRE must have unrestricted access to the board and its committees to address risks and issues identified through IRM's activities. The board of directors or the board's risk committee should receive communications from the CRE on the results of IRM's risk assessments and activities and on 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 and Audit Plans:** The board's audit committee must review and approve IA's overall charter and audit plan. *See* **page 70**.
    - The final guidelines removed the requirement to review and approve IA's risk assessments on the ground that this could impose operational burdens on the audit committee and detract from its oversight role.
  - **Oversight of CAE:** Either the audit committee or the CEO must oversee the CAE's administrative activities (instead of, as proposed, the CAE's day-to-day activities).
  - **Access by and Communications from CAE:** The CAE must have unrestricted access to the audit committee to address risks and issues identified through IA's activities. 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 IA's ability 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 providing 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 an appropriate board committee must:
  - 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 risk governance framework.
    - The final guidelines clarify that the board or board committee may rely on management to appoint the CAE and CRE(s).
  - Review and approve a written talent management program that provides for development, recruitment, and succession planning regarding the CEO, CAE and CRE, their direct reports, and other potential successors.
    - The final guidelines narrowed this responsibility from the proposed guidelines' reference to talent development, recruitment and succession planning processes for IRM, IA and individuals two levels down from the CEO.
  - Require management to assign individuals specific responsibilities within the talent management program and hold those individuals accountable for the program's effectiveness.

Davis Polk

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

- **Provide Ongoing Training to All Directors:** The board should establish and adhere to a formal, ongoing training program for all directors that considers the knowledge and experience of directors and the bank's risk profile.
  - As appropriate for the bank and 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:** Hold IRM accountable for designing the bank's written risk governance framework. *See* **page 54**.
- **Strategic Plan:** With input from the three lines of defense, be responsible for the development of a written strategic plan that contains a comprehensive assessment of risks having an impact on the bank and articulates the bank's mission statement and strategic objectives. *See* **page 56**.
- **Risk Appetite Statement:** Similarly, be responsible for the development of the bank's risk appetite statement, which must include both qualitative components and quantitative limits. *See* **page 58**.
- **Safe and Sound Risk Culture:** Help promote a safe and sound risk culture by setting an appropriate tone at the top. *See* **page 60**.
- **Oversight of FLUs and IRM:** Hold FLUs and IRM accountable for their compliance with requirements under the risk governance guidelines.
- **Resolve disagreements** between CRE and FLU executives over risk assessments.

CEO Responsibilities – Checklist *(cont.)*

- **Oversight of CAE:** If the audit committee does not have responsibility for doing so, the CEO must oversee the CAE's administrative activities, including:
  - Routine personnel matters such as leave and attendance reporting,
  - Expense account management, and
  - Other departmental matters such as furniture, equipment and supplies.
- **Oversight of CRE:**
  - The proposed guidelines would have required specific oversight by the CEO of the CRE's day-to-day activities. The OCC did not include this requirement in its final guidelines, but it noted that this expectation is implied in the CRE's reporting structure.

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.

Davis Polk

Chief Risk Executive Responsibilities – Checklist

CRE Responsibilities

- **Leadership of IRM:** Lead IRM in fulfilling its responsibilities under the risk governance framework. *See* **page 45** (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 on other matters that the CRE determines are necessary.
- **Multiple CREs:** A bank may designate one CRE, such as a chief risk officer, to oversee all IRM units, or 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.
- **No FLU Responsibilities:** A CRE should not oversee (*i.e.*, manage) any FLU.
- **Parent Company Responsibilities:** To the extent it is appropriate for a bank to incorporate or rely on components of its parent company's risk governance framework, the same individual may serve as CRE of the bank and its parent company.

Chief Audit Executive Responsibilities – Checklist

CAE Responsibilities

- **Leadership of IA:** Lead IA in fulfilling its responsibilities under the risk governance framework. *See* **page 49** (IA responsibilities).
- **Communicate to Board of Directors:** Provide information to the board's audit committee regarding the results of IA's activities and on other matters that the CAE determines are necessary.
- **No FLU Responsibilities:** A CAE should not oversee (*i.e.*, manage) any FLU.
- **Parent Company Responsibilities:** To the extent it is appropriate for a bank to incorporate or rely on components of its parent company's risk governance framework, the same individual may serve as CAE of the bank and its parent company.

Structure of the Three Lines of Defense:
Front Line Units (FLUs)

- **FLU Definition:** Any organizational unit, or a function of an organizational unit, in the bank that is (1) **accountable for a risk** that is within the scope of the risk governance guidelines (*see* **page 55**) and (2) engages in any of the following:
  - **Revenues / Expenses:** Engages in activities designed to generate revenue or reduce expenses for the parent company or bank.
  - **Operational Support:** Provides operational support or servicing to any organizational unit or function in the bank for the delivery of products or services to customers.
  - **Technology Services:** Provides technology services to any organizational unit or function covered by the risk governance guidelines.
- The revised definition of FLU clarifies that part of an organizational unit may qualify as an FLU without the rest of the organizational unit being treated as an FLU.
  - *E.g.*, Finance unit is an FLU with respect to its responsibility for overseeing cost reduction initiatives, but not with respect to its responsibility for assessing compliance with policies and procedures for preparing the bank's financial statements.

Structure of the Three Lines of Defense:
Front Line Units (FLUs) *(cont.)*

- An organizational unit that assumes responsibility for a risk created by another unit (*e.g.*, transfer of a loan portfolio) becomes an FLU.
- The revised definition of FLU also clarifies that accountability for risk is not enough without satisfying one of the additional criteria.
  - *E.g.*, Human Resources is accountable for risks related to compensation programs, but is not an FLU because it does not satisfy the additional criteria.
- An organizational unit or function that provides **legal services** will **not** ordinarily be an FLU.
  - There may be instances when a General Counsel is responsible for functions that extend beyond legal services, and these functions may be FLUs.
- **Accountability:** FLUs should be held accountable by the CEO and the board of directors for compliance with the risk governance guidelines. *See* **page 42** (FLU responsibilities).
- **No Oversight of IRM or IA:** No FLU executive should oversee IRM or IA.

Davis Polk

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.
- **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.
  - The board or the board's risk committee approves all decisions regarding the appointment or removal of the CRE(s) and approves the annual compensation and salary adjustment of the CRE(s).
  - The (each) CRE has unrestricted access to the board and its committees to address risks and issues identified through IRM's 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 45** (IRM responsibilities).

Davis Polk

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 safety and soundness regulations.
- **Independence:** IA maintains independence from FLUs and IRM through the following reporting structure:
  - The audit committee reviews and approves IA's overall charter and audit plans.
  - The audit committee approves all decisions regarding the appointment or removal of the CAE and approves the annual compensation and salary adjustment of the CAE.
  - The CAE has unrestricted access to the audit committee to address risks and issues identified through IA's activities.
  - The audit committee or the CEO oversees the CAE's administrative activities.
  - No FLU executive oversees IA.
- **Accountability:** IA should be held accountable by the CEO and the audit committee for compliance with the risk governance guidelines. *See* **page 49** (IA responsibilities).

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, either alone or in conjunction with another organizational unit that has the purpose of assisting the FLU:

- Assess, on an ongoing basis, the material risks associated with the FLU's activities and use such risk assessments as the basis for (i) fulfilling its responsibilities under the risk governance guidelines and (ii) 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 applicable risk limits have not been exceeded.
- Establish and adhere to a set of written policies that include FLU risk limits. *See* **page 63**.
  - Policies 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.

Davis Polk

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

- Establish and adhere to procedures and processes, as necessary, to maintain compliance with the written policies.
  - An FLU's processes for establishing its policies should provide for IRM's review and approval of the policies to ensure they are consistent with other policies established under the risk governance framework.
  - Within this process, IRM reviews and approves FLU's risk limits.
- 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 and distinguish breaches based on the severity of their impact on the bank. *See* **page 66** (processes governing risk limit breaches).
- Establish protocols for when and how to inform the board of directors, FLU management, IRM, IA and the OCC of a risk limit breach that takes into account the severity of the breach and its impact on the bank.

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

- ❑ Establish accountability for reporting and resolving breaches, including consequences for risk limit breaches.
- ❑ Incorporate, at a minimum, the bank's risk appetite statement, concentration risk limits and FLU risk limits into other decisions, plans, processes and programs. *See* **page 69** (relationship of risk appetite statement, concentration limits and FLU risk limits to other processes).
- ❑ Keep the board of directors informed of the bank's risk profile and risk management practices to allow the board 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 risk governance guidelines. *See* **page 72**.
- ❑ Establish and adhere to performance management and compensation programs that comply with the risk governance guidelines. *See* **page 73**.

Independent Risk Management Responsibilities – Checklist

IRM should oversee the bank's risk-taking activities and assess risks and issues independent of 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 54** (written risk governance framework).
- Identify and assess, on an ongoing basis, the bank's material aggregate risks and use these 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, applicable concentration risk limits or an FLU's risk limits have not been exceeded.

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

- Establish and adhere to enterprise policies that include concentration risk limits. *See* **page 63**.
  - Policies should state how 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, including when FLUs do not meet their responsibilities under the risk governance guidelines.

Davis Polk

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 results of monitoring to the board of directors or the board's risk committee at least quarterly. *See* **page 65** (risk appetite monitoring and communication processes).
- When necessary due to the level and type of risk, monitor FLUs' compliance with FLU risk limits, engage in ongoing communication with FLUs regarding adherence to these limits, and report any concerns to the CEO and board of directors or the board's risk committee at least quarterly.
- Identify breaches of the risk appetite statement, concentration risk limits and FLU risk limits and distinguish breaches based on the severity of their impact on the bank. *See* **page 66**.
- Establish accountability for reporting and resolving breaches, including consequences for risk limit breaches.

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

- ❑ Establish protocols for when and how to inform the board of directors, FLU management, IA and the OCC of a risk limit breach that takes into account the severity of the breach and its impact on the bank.
- ❑ Incorporate, at a minimum, the bank's risk appetite statement, concentration risk limits and FLU risk limits into other decisions, plans, processes and programs. *See* **page 69**.
- ❑ Keep the board of directors informed of the bank's risk profile and risk management practices to allow the board 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 risk governance guidelines. *See* **page 72**.
- ❑ Establish and adhere to performance management and compensation programs that comply with the risk governance guidelines. *See* **page 73**.

Internal Audit Responsibilities – Checklist

In addition to meeting the standards set forth in the OCC's existing safety and soundness regulations,* IA should ensure that the bank's risk governance framework complies with the 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 (*i.e.*, the "internal audit universe") of all of the 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.
- ❑ Establish and adhere to an audit plan that is periodically reviewed and updated that takes into account the bank's risk profile, emerging risks and issues, and establishes the frequency with which activities should be audited. *See* **page 70** (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.
  - ❑ Significant changes to the audit plan should be communicated to the board's audit committee.

Davis Polk

* *See, e.g.*, 12 CFR Part 30 Appendix A, II.B (internal audit system).

Internal Audit Responsibilities – Checklist *(cont.)*

- Report in writing conclusions, material 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 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 multiple organizational units within the bank, and
    - A determination of the effectiveness of FLUs and IRM in identifying and resolving issues in a timely manner, including the identification and mitigation of excessive risks.
  - Address potential and emerging concerns, the timeliness of corrective actions and the status of outstanding issues.
  - Reflect emerging risks and IA's assessment of the appropriateness of risk levels relative to both the quality of internal controls and the risk appetite statement.

Internal Audit Responsibilities – Checklist *(cont.)*

- Establish and adhere to processes for independently assessing the design and ongoing effectiveness of the risk governance framework on at least an annual basis.
  - The independent assessment should include a conclusion on the bank's compliance with the standards in the risk governance guidelines.
  - The final guidelines removed the requirement to include a conclusion regarding the framework's consistency 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 program 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, emerging risks and improvements in industry internal audit practices; and
  - Are consistently followed.

Davis Polk

Internal Audit Responsibilities – Checklist *(cont.)*

- ❑ Keep the board of directors informed of the bank's risk profile and risk management practices to allow the board 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 risk governance guidelines. *See* **page 72**.
- ❑ Establish and adhere to performance management and compensation programs that comply with the risk governance guidelines. *See* **page 73**.

Davis Polk

III. Risk Governance Framework:

Policies, Procedures, Processes and Programs

Davis Polk

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. The risk governance framework should include delegations from the board of directors to management committees and executive officers, as well as the risk limits established for material activities.

  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 improvements in industry risk management practices and changes in the bank's risk profile caused by emerging risks, its strategic plans or other internal and external factors.

  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 25 (board of directors responsibilities), page 33 (senior management responsibilities) and page 42 (three lines of defense responsibilities).

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

Davis Polk

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

- These categories of risk are not mutually exclusive. Any product or service may expose a bank to multiple risks and risks may also be interdependent.

Davis Polk

Written Strategic Plan

- The bank's CEO should be responsible for the development of 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 have an impact on the bank or could have an impact on the bank during the period covered by the plan;
  - Articulate an 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.
- The OCC has clarified that the risk governance guidelines do not require a specific capital plan.

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**

* The OCC provided this guidance on a bank's risk profile in the supplementary information to the proposed risk governance guidelines. The OCC did not restate this guidance with the final guidelines, but there is no indication that the OCC intended to withdraw this guidance..

Davis Polk

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. CEO CRE CAE FLUs IRM IA
  - **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.

Davis Polk

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 60** (safe and sound risk culture).
- **Quantitative limits** should:
  - Incorporate sound stress testing processes, as appropriate;
  - Address bank earnings, capital and liquidity; and
  - 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 61** (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.** Not defined in the risk governance guidelines, but the OCC clarified that it refers to shared values, attitudes, competencies and behaviors present throughout the bank that shape and influence governance practices and risk decisions.
- 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, executive management, board committees and 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 hold 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.
  - 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 and 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:
    - 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 OCC noted that 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 (*see* page 55):
  - **Concentration risk limits**; and
  - As applicable, **FLU risk limits**.
- 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.
- Concentration and FLU risk limits should limit excessive risk taking and, when aggregated across FLUs, provide that these risks do not exceed the limits established in the bank's risk appetite statement.

Davis Polk

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 concentrations of risk.
- Concentrations of risk can arise in any risk category, *e.g.,* 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 causes 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**

Davis Polk

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:

CEO CRE FLUs IRM

- Identify breaches of the risk appetite statement, concentration risk limits and FLU risk limits.
- 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, IA and the OCC of a risk limit breach that takes into account the severity of the breach and its impact on the bank.
  - 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.
- 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, procedures and processes designed to provide risk data aggregation and reporting capabilities are appropriate for the size, complexity, and risk profile of the bank and to 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 support 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.

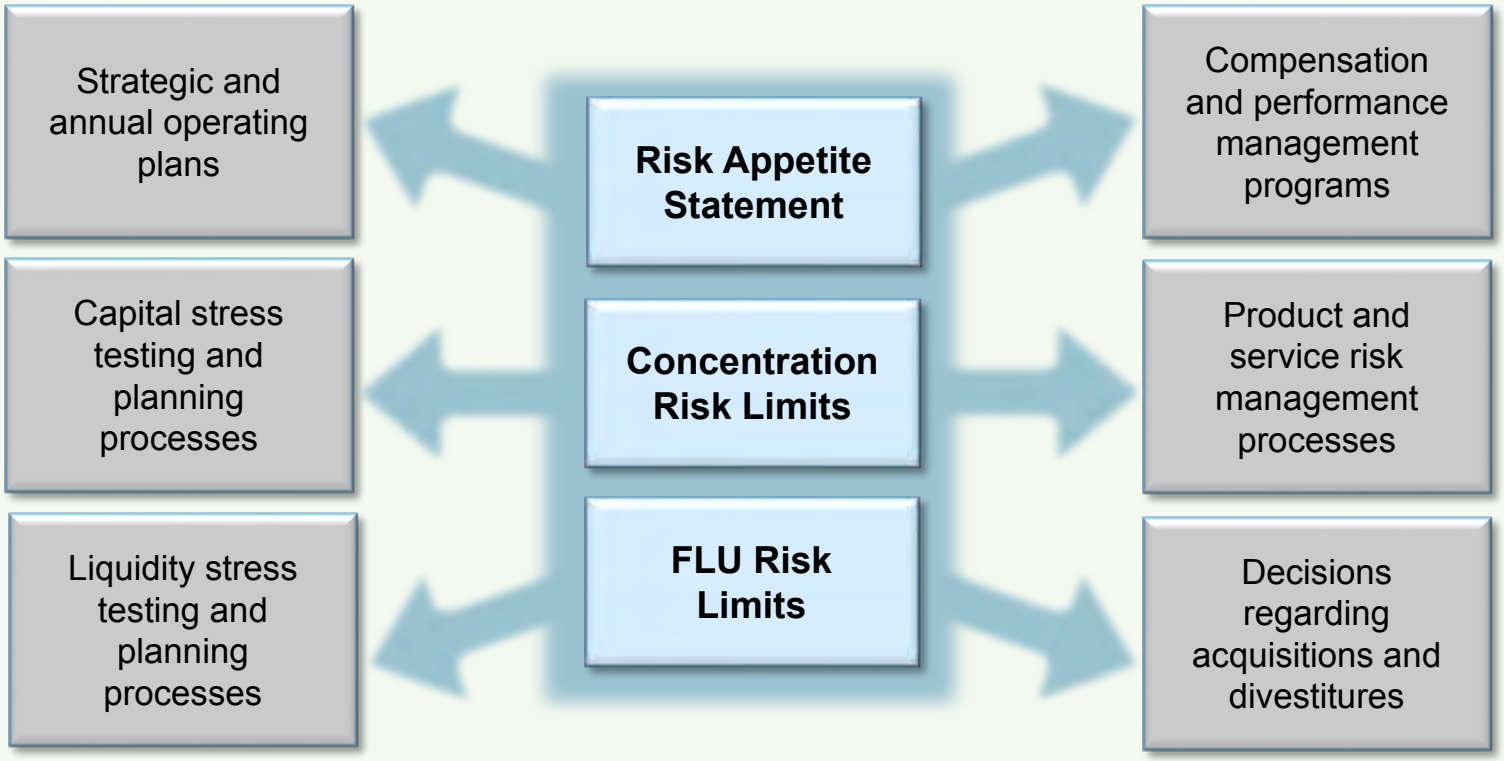
Risk Data Aggregation and Reporting:
OCC's Expectations for G-SIBs

- 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.
- In the supplementary information to the proposed risk governance guidelines, the OCC announced that it 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.

Davis Polk

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

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



Davis Polk

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 processes, product lines, services and functions that serve as the basis for the audit plan and assess the associated risks, including emerging risks.
  - IA can leverage risk assessments conducted by FLUs or IRM in deriving risk assessments, but IA should apply independent judgment.
  - IA may periodically adjust its risk assessments based on changes in the bank's strategy and the external environment
- **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 report discrepancies in IA's risk ratings and FLU and IRM risk ratings to the audit committee.

Audit Plan *(cont.)*

- **Contents of the Audit Plan** *(cont.)*:
  - Include ongoing monitoring to identify emerging risks and ensure that units, product lines, services and functions that receive a low risk rating are re-evaluated with reasonable frequency.
  - 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.
    - Evaluation should include reputation and strategic risk, along with IRM and traditional risks.
- **Updates to the Audit Plan**
  - The audit plan should be periodically reviewed and updated.
  - Significant changes to the audit plan should be communicated to the audit committee.

Audit Comm. CAE IA

Davis Polk

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.
- The board of directors or any appropriate committee should: **Board** / **Board Comm.**
  - 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 risk governance framework.
    - The final guidelines clarify that the board or board committee does not need to be involved in the hiring process for the CAE and CRE(s) – they may rely on management.
  - Review and approve a written talent management program that provides for development, recruitment, and succession planning regarding the CEO, CAE and CRE(s), their direct reports, and other potential successors.
    - The final guidelines remove reference to oversight of development, recruitment and succession planning for IRM, IA and individuals two levels down from the CEO.
  - 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

A bank should establish and adhere to compensation and performance management programs that comply with 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, as well as the timeliness of corrective action to resolve such issues and concerns.
- Attract and retain the talent needed to design, implement and maintain an effective risk governance framework.
- 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.
- The OCC noted that compensation practices are also addressed by its safety and soundness regulations, the federal banking agencies' 2010 guidance on incentive compensation, and Dodd-Frank Act Section 956.

Davis Polk

IV. Risk Governance Framework:

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

Davis Polk

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 in its entirety, without modification, 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 reported on the call reports for the four most recent consecutive quarters, the bank's average total consolidated assets represent **≥ 95%** of the parent company's; or
    - The bank demonstrates in a written analysis submitted to and approved by 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.
    - This assessment should be conducted at least annually, in conjunction with IRM's review and update of the risk governance framework.

A Bank Must Generally Develop Its Own Risk Governance Framework *(cont.)*

- Even if a bank is permitted to use its parent's risk governance framework, the bank's board must:
  - Review the bank's risk appetite statement, which must document any adjustments that are necessary or material differences between the risk profiles of the bank and parent; and
  - Approve the bank's risk appetite statement.

Using Components of Parent Company's Risk Governance Framework

- If a bank's risk profile is **not** substantially the same as its parent's risk profile, the bank may, in consultation with the OCC, incorporate and rely on components of the parent company's risk governance framework when developing its own risk governance framework, provided those components are consistent with the objectives of the risk governance guidelines.
- In this case, 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 and management, including:
    - Ensuring that assets and businesses are not transferred into the bank from non-bank entities without proper due diligence, and
    - Ensuring that complex booking structures established by the parent company protect the safety and soundness of the bank.
- The bank should consult with OCC examiners to determine which components of a parent company's risk governance framework may be used to ensure that the bank's risk governance framework complies with the OCC's guidelines.

Dual-Hatted Employees

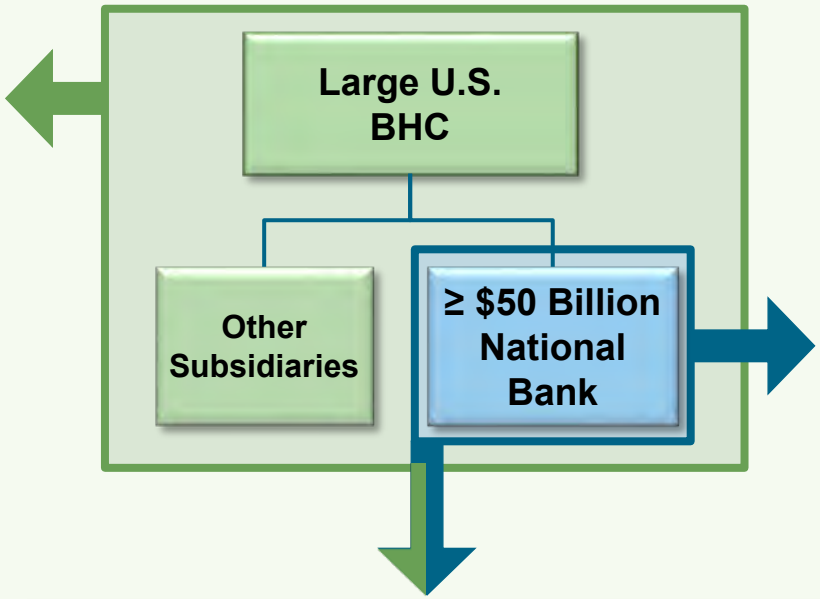
- The OCC encourages banks to leverage their parent company's risk governance framework to the extent possible, including using parent company employees.
- A bank's CRE may be an employee of both the bank and the bank's parent company.
  - When a bank's CRE is also a parent-company employee, the CRE may report to a parent company executive, provided that the parent company executive does not impede the CRE's independence in the bank's risk governance framework.
- In addition, it may be appropriate for the same individual to serve as the CRE or CAE of both the bank and its parent company.

OCC Guidelines and Dodd-Frank Enhanced Prudential Standards for Large U.S. BHCs

Federal Reserve's Enhanced Prudential Standards for Large BHCs

Requires a U.S. BHC with ≥ $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 approve and periodically review the BHC's enterprise-wide risk management practices.
- Must appoint a chief risk officer with specified enterprise-wide risk management responsibilities.



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

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.

Davis Polk

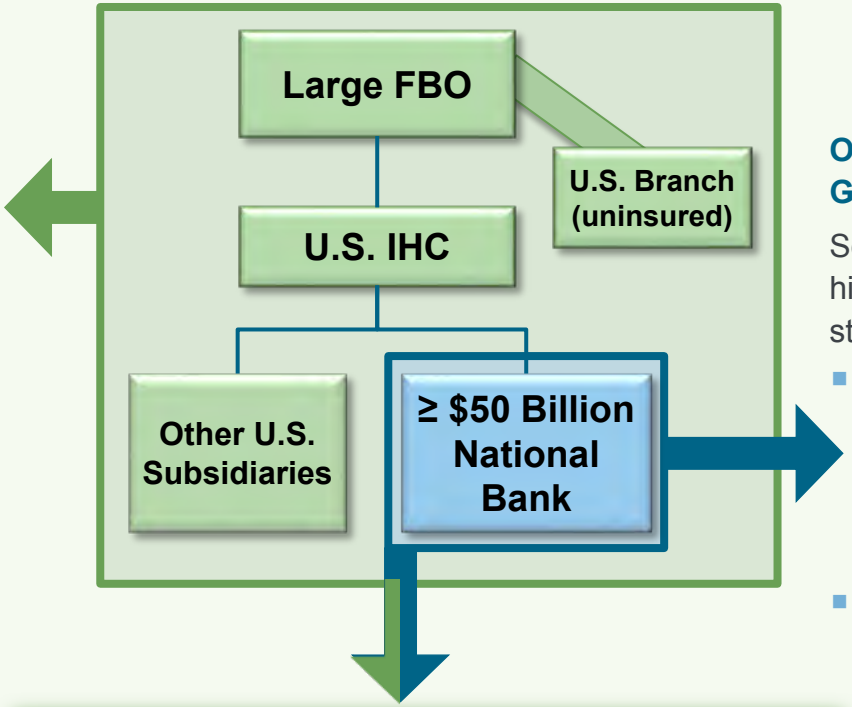
Click here to return to table of contents

OCC Guidelines and Dodd-Frank Enhanced Prudential Standards for Large FBOs

Federal Reserve's Enhanced Prudential Standards for Large FBOs

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

- Must establish a U.S. risk committee, generally within the board of directors of either the FBO or the U.S. intermediate holding company (IHC).
- U.S. risk committee must approve and periodically review the risk management policies 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.



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

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.

Davis Polk

Click here to return to table of contents

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.

Luigi L. De Ghenghi	212 450 4296	luigi.deghenghi@davispolk.com
Randall D. Guynn	212 450 4239	randall.guynn@davispolk.com
Margaret E. Tahyar	212 450 4379	margaret.tahyar@davispolk.com
Christopher M. Paridon	202 962 7135	christopher.paridon@davispolk.com
Andrew S. Fei	212 450 4063	andrew.fei@davispolk.com
Michael I. Overmyer	212 450 4408	michael.overmyer@davispolk.com
Jennifer E. Kerslake	212 450 6259	jennifer.kerslake@davispolk.com

Davis Polk