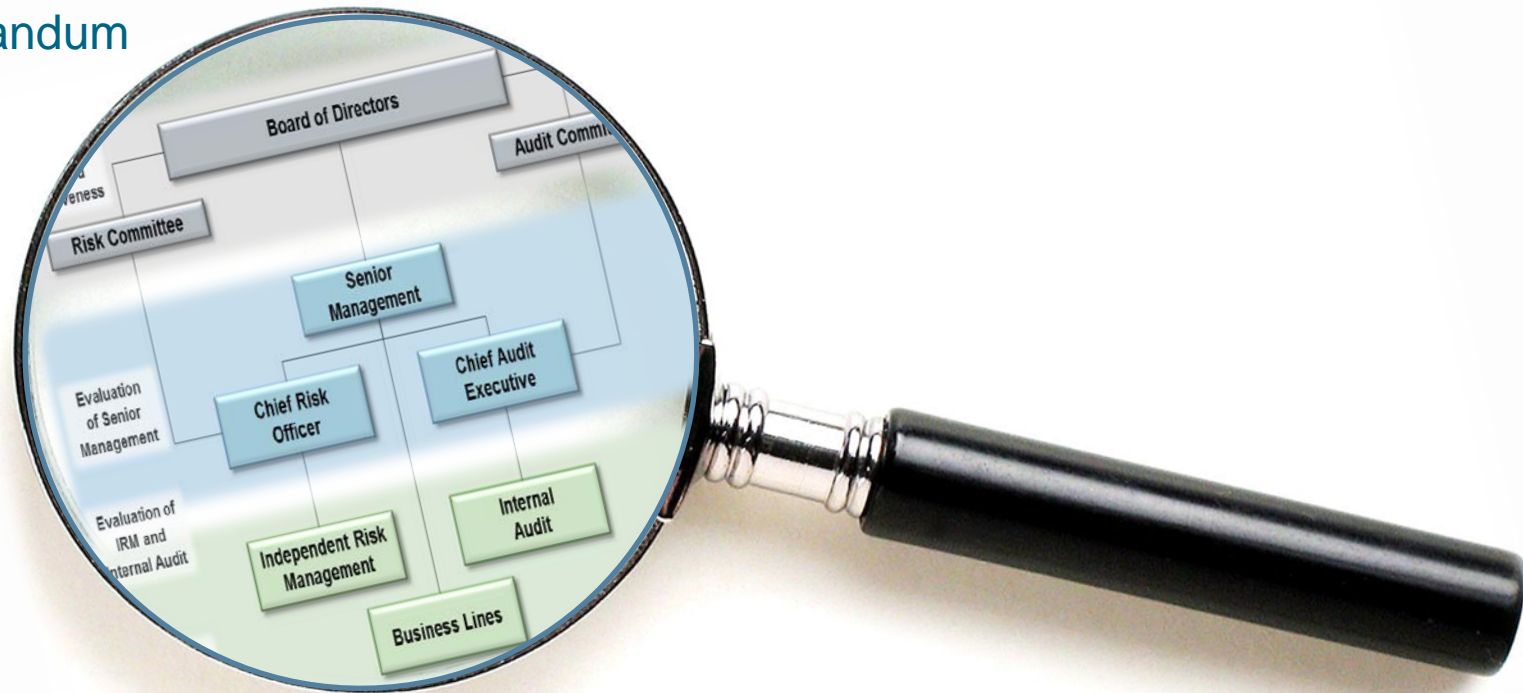


# Corporate Governance and Controls: The Federal Reserve's Governance and Management Proposals—Application to a Large U.S. Financial Institution

## Visual Memorandum



June 5, 2018


**Davis Polk**

Davis Polk & Wardwell LLP

© 2018 Davis Polk & Wardwell LLP | 450 Lexington Avenue | New York, NY 10017

This communication, 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. This may be considered attorney advertising in some jurisdictions. Please refer to the firm's [privacy policy](#) for further details.

# Table of Contents

Click on an item to go to that page 

|   |    |
|---|----|
| <a href="#"><u>Background and Overview</u></a>                                    | 3  |
| <a href="#"><u>Federal Reserve Corporate Governance Review</u></a>                | 6  |
| <a href="#"><u>Proposed Board Effectiveness Guidance</u></a>                      | 7  |
| <a href="#"><u>Proposed Guidance on Communication of Supervisory Findings</u></a> | 14 |
| <a href="#"><u>LFI Rating System – Governance and Controls Component</u></a>      | 15 |
| <a href="#"><u>Supervisory Expectations – Senior Management</u></a>               | 17 |
| <a href="#"><u>Supervisory Expectations – Business Line Management</u></a>        | 22 |
| <a href="#"><u>Supervisory Expectations – IRM and Controls</u></a>                | 30 |
| <a href="#"><u>Davis Polk Contacts</u></a>  | 41 |

For in-depth discussion of the Federal Reserve’s **proposed LFI rating system**, please see our companion visual memorandum

# Background and Overview

- The Federal Reserve has proposed new supervisory guidance on corporate governance (**Governance Proposal**) that would apply to large U.S. financial institutions
- As discussed in our companion visual memorandum, the Federal Reserve in August also proposed a new supervisory rating system for large financial institutions (**LFIs**)
  - The LFI rating system includes a **Governance and Controls** component that would evaluate the effectiveness of a firm's board of directors, its management of business lines, its internal risk management, its internal controls and, for U.S. G-SIBs, its recovery planning
- The Federal Reserve released proposed supervisory guidance for senior management, business line management, independent risk management (IRM) and internal controls for LFIs in early January 2018 (the **Management Guidance**)
- Although there were certain variations among the proposals, each generally set applicability thresholds at asset sizes of \$50 billion or greater. We expect that, in light of the passage of the Bipartisan Banking Act, the final versions of the proposals will adjust those thresholds upwards. Our visual memorandum on the Bipartisan Banking Act is available [here](#)

# Background and Overview

- The comment deadline for the August proposals was extended to February 15, 2018 and the comment deadline for the January proposal was March 15, 2018.
- In the Management Guidance, the Federal Reserve states that it “expects to finalize the proposed guidance for use in assigning initial ratings under the LFI rating system beginning in 2018.”

For additional commentary on the Governance Proposal, please see our public client memorandum from August, [available here](#)

For additional commentary on the Management Guidance, please see our blog post from January, [available here](#)

# Background and Overview

- The Governance Proposal was informed by the Federal Reserve’s **multi-year review** of the practices of boards of directors, particularly at the largest banking organizations
  - Jerome Powell, President Trump’s nominee to be the next Chair of the Federal Reserve, stated in the spring of 2017 that boards must be able to “focus on setting the overall strategic direction of the firm, while overseeing and holding senior management accountable” rather than being distracted “by an overly detailed checklist of supervisory process requirements.”
- The Governance Proposal consists of **three components**:
  - A proposed process for a **comprehensive review** of supervisory expectations and regulatory requirements
  - The proposed **board effectiveness guidance**; and
  - The proposed guidance on **communication of supervisory findings**

# Federal Reserve Corporate Governance Review

## Comprehensive Review of All Existing Supervisory Expectations and Regulatory Requirements

- As part of its proposal, the Federal Reserve is conducting a **comprehensive review of all existing supervisory expectations** and **regulatory requirements** relating to boards of directors of all BHCs and SLHCs so that “unnecessary, redundant or outdated” expectations may be revised or eliminated
- The **first phase** of the Federal Reserve’s corporate governance review has identified 27 SR letters for revision or elimination
- The **second phase** of the Federal Reserve’s review will focus on regulations and interagency guidance
  - This phase will take more time to complete, and proposed changes would be released for notice and comment at a later date

# Proposed Board Effectiveness Guidance

## Board Effectiveness

- The board effectiveness guidance would clarify supervisory expectations for boards as distinct from expectations for senior management and identifies **five key attributes** of effective boards that would be used to assess the board of a large financial institution

## No One-Size-Fits-All

- The Federal Reserve acknowledges that applying standardized expectations for boards fails to take into account differences in firms' operations, risk profiles and complexity, and potentially prevents a board from achieving maximum effectiveness in meeting its core responsibilities

## Interaction with OCC Requirements

- The Governance Proposal applies only at the bank holding company level
  - The proposal's interaction with OCC requirements for national bank boards is uncertain; this is a key issue for many U.S. G-SIBs because the boards of many BHCs and their national banks overlap

### Five Key Attributes

1. **Set clear, aligned and consistent direction regarding firm's strategy and risk tolerance**
2. **Actively manage information flow and board discussions**
3. **Hold senior management accountable**
4. **Support the independence and stature of the firm's independent risk management and internal audit functions**
5. **Maintain a capable board composition and governance structure**

# Proposed Board Effectiveness Guidance

## THE ROLE OF BOARD SELF-ASSESSMENT

- Under the Governance Proposal, a board is encouraged to provide a **self-assessment** of its effectiveness, which the Federal Reserve would take into consideration in its evaluation
  - The Federal Reserve requested comment regarding whether boards should be required to perform a self-assessment and provide the results to the Federal Reserve
- A number of industry comment letters requested that the Federal Reserve not require self-assessments or submission of such self-assessments to the Federal Reserve
  - Responsible banking boards already conduct self-assessments in a manner that best suits the firm's nature and culture, recognizing that a proper self-assessment is a **highly sensitive exercise** that balances candor with respect
  - Requiring a self-assessment will lead to an **overly prescriptive de facto standard** and requiring that the results be shared with the Federal Reserve may chill candor and undermine the effectiveness of the self-assessment



# Proposed Board Effectiveness Guidance

## ATTRIBUTE #1 – SET CLEAR, ALIGNED AND CONSISTENT DIRECTION

- An effective board guides and approves the firm’s strategy and sets its risk tolerance
  - The strategy and risk tolerance should be clear and aligned, and include a long-term perspective on risks and rewards that is consistent with the capacity of the firm’s risk management framework
- The firm’s **strategy** should be detailed enough for senior management to:
  - Identify the firm’s strategic objectives;
  - Create effective operating structures (including implementation strategies, plans and budgets) for each business line; and
  - Establish effective audit, compliance, and risk management and control functions
- The firm’s **risk tolerance** should be detailed enough for the chief risk officer (CRO) and the independent risk management function (IRM) to set firm-wide risk limits
- Prior to approving the firm’s “**significant policies, programs and plans**,” the board should assess whether they are consistent with the firm’s strategy, risk tolerance and risk management capacity

### Significant policies, programs and plans include the following:

- Capital plan
- Recovery and resolution plans
- Audit plan
- Enterprise-wide risk management policies
- Liquidity risk management policies
- Compliance risk management program
- Incentive compensation and performance management programs

# Proposed Board Effectiveness Guidance

## ATTRIBUTE #2 – ACTIVELY MANAGE INFORMATION FLOW AND BOARD DISCUSSIONS

- An effective board actively **manages its information flow** and its deliberations so it can make sound, well-informed decisions in a manner that meaningfully takes into account risks and opportunities
  - Board should direct senior management to provide information that is timely and accurate, with the appropriate level of detail and context to enable the board to make sound, well-informed decisions
  - Board should have practices and processes in place to evaluate information flows and engage senior management on improvements
- Directors may **seek additional information** about the firm and its activities, risk profile, talent, and incentives outside routine board and committee meetings
- Directors should take an active role in **setting board meeting agendas** such that the content, organization, and time allocated to each topic allows the board to discuss strategic tradeoffs and to make sound, well-informed decisions

### How to Obtain Additional Information?

- Special sessions of the board
- Outreach to staff other than the Chief Executive Officer and his or her direct reports
- Discussions with senior supervisors
- Training on specialized topics

# Proposed Board Effectiveness Guidance

## ATTRIBUTE #3 – HOLD SENIOR MANAGEMENT ACCOUNTABLE

- An effective board **holds senior management accountable** for implementing the firm’s strategy and risk tolerance and maintaining the firm’s risk management and control framework
- An effective board should **actively engage** senior management by structuring sufficient time in board meetings, encouraging diverse views and challenging senior management when warranted
- **Independent directors** should be sufficiently empowered to serve as a **check on senior management**
- An effective board should engage in robust and **active inquiry** into areas such as current and emerging risks; strategy and risk tolerance for relevant lines of business; material or persistent deficiencies in risk management and controls; and performance and compensation programs that encourage prudent risk taking
- An effective board should evaluate the **performance and compensation** of senior management
  - Board should establish and approve clear financial and nonfinancial performance objectives that are aligned with the firm’s strategy and risk tolerance for the CEO, CRO and Chief Audit Executive (CAE) and other members of senior management as appropriate
- An effective board should approve and periodically reassess **succession plans** for the CEO and, as needed, the CRO and CAE
  - Succession plans for other members of senior management, such as the CFO, may be warranted

**Senior management** refers to the core group of individuals who are directly accountable to the board for the sound and prudent day-to-day management of the firm

# Proposed Board Effectiveness Guidance

## ATTRIBUTE #4 – SUPPORT THE INDEPENDENCE AND STATURE OF IRM AND INTERNAL AUDIT

- Risk and audit committees should **support the independence and stature of the IRM and internal audit functions**
  - An effective board should be able to identify instances where the independence and stature of IRM or internal audit have materially impacted business deliberations, decisions, practices, and/or the firm’s strategy
- **Risk committee** should:
  - Communicate directly with the CRO on material risk management issues;
  - Review IRM’s budget, staffing, and systems;
  - Provide IRM with direct and unrestricted access to the risk committee;
  - Direct the appropriate inclusion of IRM representatives on senior management-level committees; and
  - Be able to effect changes that align with the firm’s strategy and risk tolerance
- **Audit committee** should:
  - Meet directly with the CAE regarding the internal audit function;
  - Support internal audit’s budget, staffing, and systems relative to the firm’s size and complexity and the pace of technological and other changes; and
  - Review the status of recommendations to remediate deficiencies and supervisory findings

**Active engagement** by directors on the risk committee and audit committee entails inquiring into (among other things):

- Material or persistent breaches of risk appetite and risk limits;
- Timely remediation of material or persistent internal audit and supervisory findings; and
- Appropriateness of the annual audit plan

# Proposed Board Effectiveness Guidance

## ATTRIBUTE #5 – MAINTAIN A CAPABLE BOARD COMPOSITION AND GOVERNANCE STRUCTURE

- An effective board has a **composition, governance structure, and established practices** that are appropriate for the firm’s size, complexity, operations and risk profile, as they change over time
- Directors should have a **diversity of skills, knowledge, experience, and perspectives**
  - The process for identifying and selecting director nominees should consider a potential nominee’s expertise, availability, integrity, and potential conflicts of interest
- An effective board’s **governance structure** should be capable of overseeing and addressing issues arising from the firm’s size, operations, activities, risk profile, and resolvability
  - Board should engage third-party advisors and consultants, when appropriate, to supplement its knowledge, expertise and experience
- An effective board should conduct a **self-assessment** of its strengths and weaknesses, including the performance of the board committees, particularly the risk, audit, and other key committees

**Governance structure** refers to the structure of board committees and to management-to-committee reporting lines

As noted above, the industry has questioned the appropriateness of de facto standards for self-assessments

# Proposed Guidance on the Communication of Supervisory Findings

- This proposed guidance would revise the process by which Federal Reserve staff communicate **supervisory findings** to all firms
- Under the proposal, Federal Reserve supervisory staff would typically **direct MRIAs and MRAs to senior management**, rather than to the board, and senior management would be responsible for keeping the board informed of its efforts to remediate MRIAs and MRAs
- Supervisory staff would direct MRIAs and MRAs to the board itself, or an executive-level board committee, only when either:
  - The supervisory finding relates to significant weaknesses in the board's governance structure or practices; or
  - Senior management has failed to take appropriate remedial action with respect to a supervisory finding that was originally addressed to senior management

**Supervisory findings** mean Matters Requiring Immediate Attention (MRIAs) and Matters Requiring Attention (MRAs)

# LFI Rating System – Governance and Controls Component

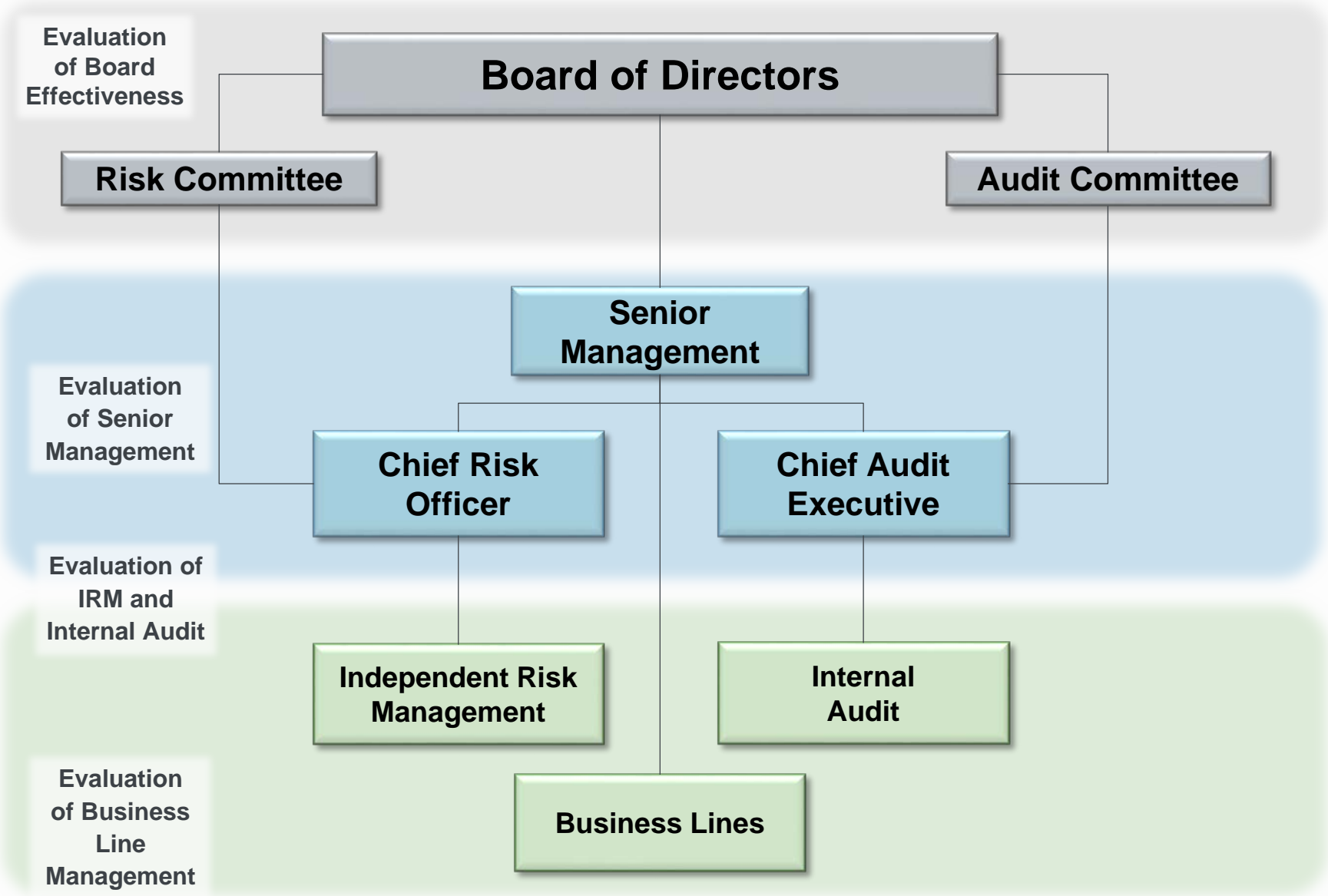
## OVERVIEW

### Supervisory Expectations

- The supervisory assessment of an LFI's management of business lines and of IRM and controls would have three elements:
  - Expectations for **senior management** with respect to both business lines and IRM and controls;
  - Expectations for the **management of business lines**; and
  - Expectations for **IRM and controls**
- The discussion on the following pages is based on the Management Guidance proposed by the Federal Reserve in January 2018
  - If the LFI rating system is finalized before the Management Guidance is finalized, firms would be evaluated using existing supervisory guidance until Management Guidance is finalized

# Governance and Controls Component

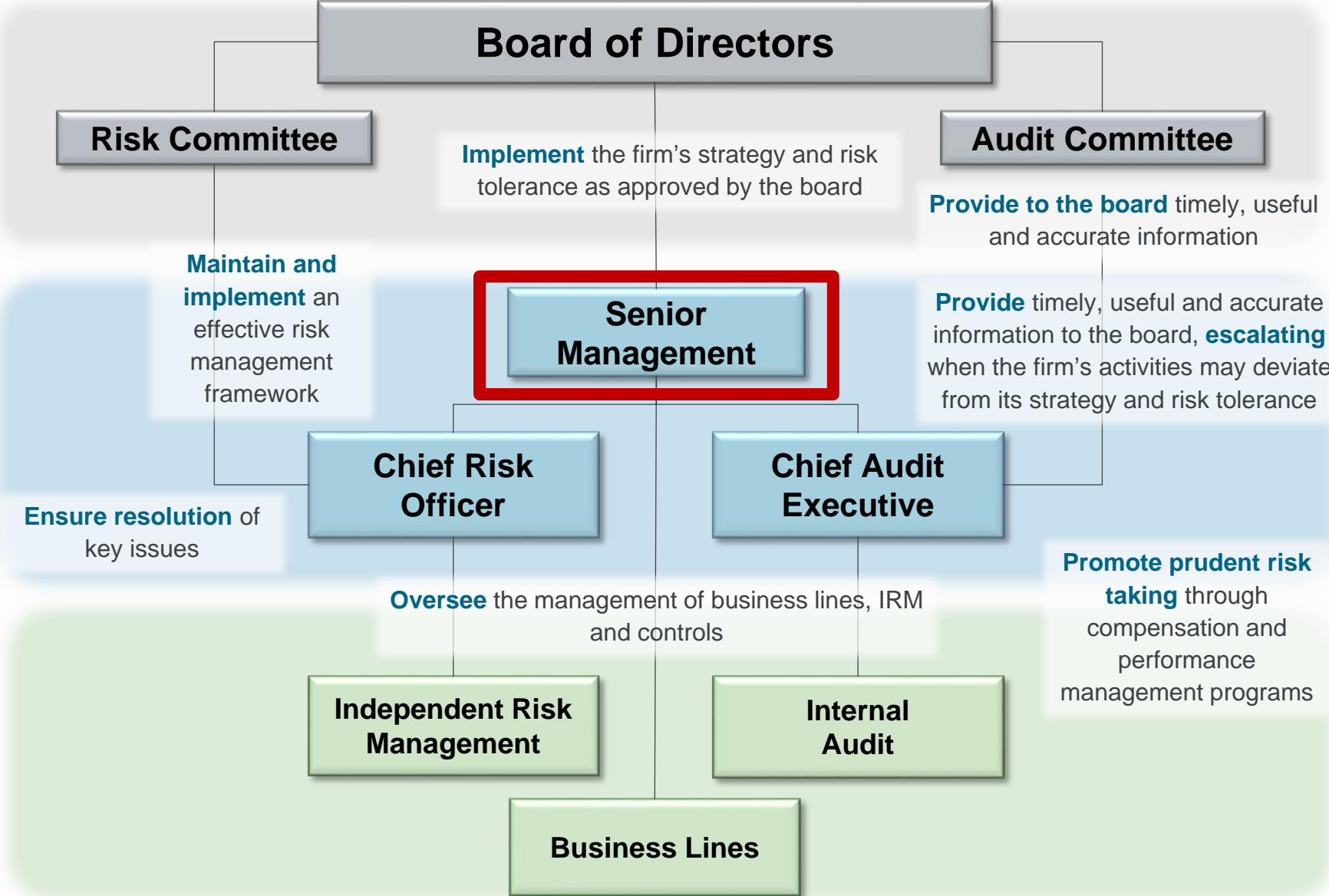
## OVERVIEW





# Governance and Controls Component

## SUPERVISORY EXPECTATIONS – SENIOR MANAGEMENT



# Governance and Controls Component

## SUPERVISORY EXPECTATIONS – SENIOR MANAGEMENT

### Implementation of firm strategy and risk tolerance as approved by the firm's board

- Implement the strategic and risk objectives across the firm so that they support the firm's long-term resiliency and safety and soundness, including the firm's resilience to a range of stressed conditions
- Ensure that the firm's infrastructure, staffing, and resources are sufficient to carry out the firm's strategy and manage the firm's activities in a safe and sound manner, and in compliance with applicable laws and regulations, including those related to consumer protection, as well as policies, procedures, and limits.
- Identify when there is a risk that the firm's activities collectively may deviate from the firm's strategy and risk tolerance and escalate such instances to the board of directors

**Risk tolerance** means the aggregate level and types of risk the board and senior management are willing to assume to achieve the firm's strategic business objectives, consistent with applicable capital, liquidity, and other requirements and constraints.

**Risk objectives** are the level and type of risks a business line plans to assume in its activities relative to the level and type specified in the firmwide risk tolerance.

# Governance and Controls Component

## SUPERVISORY EXPECTATIONS – SENIOR MANAGEMENT

### Maintenance and implementation of effective risk management framework

- Ensure that the firm appropriately manages risk consistent with its strategy and risk tolerance
- Establish clear responsibilities and accountability for identifying, measuring, managing and controlling risk
- Promote and enforce prudent risk-taking behaviors and business practices, including through the firm's compensation and performance management systems
- Develop and maintain the firm's policies and procedures and system of internal controls, commensurate with the firm's size, scope of operations, activities, and risk profile, to ensure compliance with laws and regulations and consistency with supervisory expectations
- Periodically assess the risk management framework as a whole to ensure that it remains comprehensive and appropriate and has kept pace with changes in the business line's products, services, and activities as well as changes in economic conditions and the broader market environment

**Internal controls** are the policies, procedures, systems and processes designed to provide reasonable assurance regarding:

- Effectiveness and efficiency of operations
- Reliability of financial reporting (including risk reporting)
- Compliance with laws and regulations (including those related to consumer protection)
- Safeguarding of assets and information.

# Governance and Controls Component

## SUPERVISORY EXPECTATIONS – SENIOR MANAGEMENT

### Oversight and management of business lines and IRM and controls

- Assessing the effectiveness of senior management would include senior management's role in managing the firm's day-to-day operations, promoting safety and soundness and compliance with internal policies and procedures, laws, and regulations, including those related to consumer protection
- Decisions by senior management should be based on a full understanding of the firm's risks and activities

Firms should have **robust mechanisms** in place that allow senior management to:

- Keep apprised of drivers and trends related to current and emerging risks, material limit breaches, and other material issues
- Maintain and assess the firm's system of internal controls
- Stay informed about material deficiencies and limitations in risk management and control practices, and ensure that such deficiencies are remediated in a timely fashion
- Assess the potential impact of the firm's activities and risk positions on the firm's capital, liquidity, and overall risk profile
- Assess the firm's financial and nonfinancial performance relative to the firm's strategy and risk objectives
- Maintain robust management information systems to support oversight of the firm's activities and risk positions, and to provide information to the board
- Maintain current succession and contingency staffing plans for key positions.

# Governance and Controls Component

## SUPERVISORY EXPECTATIONS – SENIOR MANAGEMENT

### Ensure effective firm-wide communication and information sharing

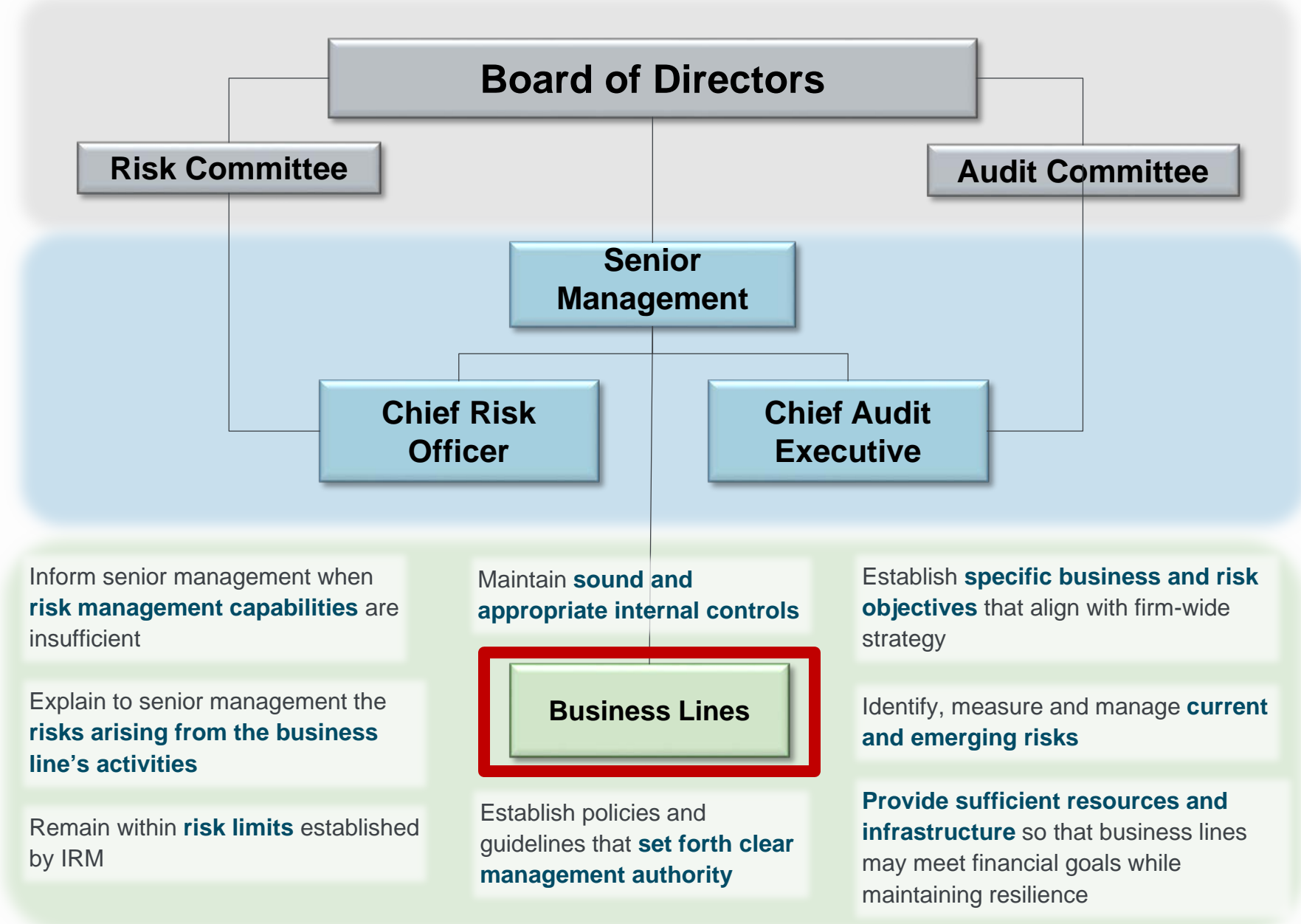
- Address any impediments to the effective flow of information, including those that could result in decisions being made or actions being taken in isolation

### Provide timely, useful and accurate information to the board

- Be responsive to direction from the board and to the board's informational needs
- Ensure resolution of risk management issues (including those identified by the firm and outstanding supervisory matters), escalate issues to the board, and communicate issues internally when appropriate
- Report regularly to the board on responses to, and remediation of:
  - Material audit and supervisory findings
  - Risk management and control deficiencies
  - Material compliance issues (including those related to consumer protection)
  - The outcomes of risk reviews which may result in remedial actions

# Governance and Controls Component

## SUPERVISORY EXPECTATIONS – BUSINESS LINE MANAGEMENT



# Governance and Controls Component

## SUPERVISORY EXPECTATIONS – BUSINESS LINE MANAGEMENT

### Which Business Lines Would Be Subject to the Management Guidance?

- For G-SIBs and certain other LFIs, the Management Guidance would apply to **all business lines**
- The Federal Reserve stated that all expectations for the management of business lines also apply to critical operations, which are central to its supervisory focus

### Who Is Business Line Management?

- Business line management refers to the core group of individuals responsible for prudent day-to-day management of a business line and accountable to senior management for that responsibility. Depending on a firm's organizational structure, business line management may or may not be members of senior management
- If management of a business line is not a member of senior management, business line management is responsible for fully engaging senior management, so that senior management can effectively carry out its responsibilities

**Business line** means a defined unit or function of a financial institution, including associated operations and support that provides related products or services to meet the firm's business needs and those of its customers.

# Governance and Controls Component

## SUPERVISORY EXPECTATIONS – BUSINESS LINE MANAGEMENT

### Execute business line activities consistent with the firm's strategy and risk tolerance

- Establish specific business and risk objectives for each business line that align with the firmwide strategy and risk tolerance
- Inform senior management when the business line's risk management capabilities are insufficient to achieve those business and risk objectives
- During the strategic planning process with senior management, clearly present the risks emanating from the business line's activities
  - Business line management should explain how those risks are managed and align with the firm's risk tolerance
- Provide information to senior management regarding the business line's current and potential risk profile and its alignment with the firm's risk tolerance
  - Information reported should enable senior management to make critical decisions about the business line's strategic direction and risks



# Governance and Controls Component

## SUPERVISORY EXPECTATIONS – BUSINESS LINE MANAGEMENT

### Identify, measure, and manage current and emerging risks that stem from business line activities and external conditions

- Ensure that risk assessments include all relevant risks, both financial and non-financial, including compliance risk, and on-balance and off-balance sheet significant exposures and activities
- In measuring risks, consider the size and risk characteristics of the business line's exposures and activities
  - Understand risks affecting the business line as a whole as well as its segments
- Incorporate appropriate feedback from IRM on business line risk positions, implementation of the risk tolerance, and risk management practices
- Manage the business line's activities so they remain within risk limits established by IRM
  - Consult with senior management before allowing any exceptions to risk limits and subject any exceptions to the firm's formal approval process
- Adhere to the firm's policies and procedures for vetting new products and initiatives and escalate to senior management any required changes to risk management systems or internal control policies and procedures arising from a new business or initiative
  - Growth in a new business should be consistent with the firm's risk management capabilities

**Emerging risks** include those that have yet to create a material impact or would only arise during stressful or unlikely circumstances.

# Governance and Controls Component

## SUPERVISORY EXPECTATIONS – BUSINESS LINE MANAGEMENT

### **Provide a business line with sufficient resources and infrastructure to meet strategic objectives while maintaining financial and operational strength and resilience over a range of operating conditions**

- Resources and infrastructure should include:
  - Management information systems that are sufficiently flexible to produce ad hoc and more frequent reporting when necessary
  - Clearly defined staff roles and responsibilities for key positions, as well as management reporting lines
  - Appropriate separation of duties and internal controls for effectively managing risk associated with its business strategy
  - Staff with skills and experience commensurate with the business line's activities and risks
  - Succession and contingency plans for key positions
  - Training and development for staff to ensure sufficient knowledge of business line activities; compliance, operations and risk management processes; controls; and business continuity

### **Financial strength and resilience**

means maintaining effective capital and liquidity governance and planning processes, and sufficiency of related positions, to provide for continuity of the consolidated organization and its core business lines, critical operations, and banking offices through a range of conditions

### **Operational strength and resilience**

means maintaining effective governance and controls to provide for continuity of the consolidated organization and its core business lines, critical operations, and banking offices, and promote compliance with laws and regulations, including those related to consumer protection, through a range of conditions

# Governance and Controls Component

## SUPERVISORY EXPECTATIONS – BUSINESS LINE MANAGEMENT

**Provide a business line with sufficient resources and infrastructure to meet strategic objectives while maintaining financial and operational strength and resilience over a range of operating conditions**

- Inform senior management if the business line's resources and infrastructure are insufficient to meet business objectives in a safe and sound manner
- Reinforce balanced risk-taking and provide incentives for appropriate behaviors through talent management processes, compensation arrangements, and other performance management processes

# Governance and Controls Component

## SUPERVISORY EXPECTATIONS – BUSINESS LINE MANAGEMENT

### Develop and maintain an effective system of sound and appropriate internal controls that helps to ensure legal and regulatory compliance and to support effective risk management

- Regularly test to ensure the controls within the business line are functioning as expected and are effective in managing risks
  - More frequent testing is appropriate for key controls, or controls that have undergone a material change
- Ensure that deficiencies in control design and operating effectiveness are remediated
- Provide periodic reports on the operation of controls to senior management and escalate to senior management material internal control deficiencies and any systematic control violations
- Reassess all key controls periodically to ensure relevancy and alignment with current approved policies

A business line's **system of controls** should include:

- access controls;
- change controls; and
- data integrity controls, including data reconciliations, variance analysis and data quality logic checks

# Governance and Controls Component

## SUPERVISORY EXPECTATIONS – BUSINESS LINE MANAGEMENT

**Establish policies and guidelines that delineate accountability, set forth clear lines of management authority within the business line and align desired behavior with the firm's performance management incentives**

- Actively supervise employees in light of the firm's policies and guidelines
- Hold employees accountable for conduct that is inconsistent with board and senior management directives and inform senior management as appropriate
- Ensure that training for new and existing employees explicitly addresses and emphasizes the importance of professional conduct and compliance with laws and regulations, including those related to consumer protection
- Have ongoing and effective means to prevent, detect, and remediate risk management and compliance failures of business line policies and procedures, as well as policies and limits established by the firm's senior management
- Put in place indicators and early warning mechanisms to facilitate timely detection of existing and potential issues

# Governance and Controls Component

## SUPERVISORY EXPECTATIONS – IRM AND CONTROLS

- The evaluation of an LFI's IRM and controls would focus on four areas:
  - Governance, independence and stature, including the CRO and CAE;
  - The IRM function, including risk tolerance and limits;
  - Internal controls; and
  - Internal audit
- The Federal Reserve's supervisory expectations for these areas are discussed on the following pages

### The Concept of Stature

**Stature** refers to the ability and authority to influence decisions and effect change throughout the organization, procure resources necessary to carry out responsibilities, escalate issues as needed to senior management and the board, and observe or participate on relevant management committees.

# Governance and Controls Component

SUPERVISORY EXPECTATIONS – GOVERNANCE, INDEPENDENCE AND STATURE - CRO

## Board of Directors

Inform the board of directors when

- his or her stature, independence, or authority is not sufficient to provide objective and independent assessments of the firm's risks
- activities or practices do not align with the overall risk tolerance

## Risk Committee

**Report directly** to the board's risk committee and the CEO; provide reports to the risk committee at least quarterly

Possess **capability and experience** in identifying, assessing, and managing risk exposures of large, complex financial institutions

**Periodically assess** whether IRM has appropriate staffing and systems, sufficient understanding of risks, and sufficient authority to escalate deficiencies and challenge management

**Support IRM's independence** from the business lines

## Audit Committee

**Provide** relevant risk information and **recommend constraints** on risk-taking and enhancements to risk practices to senior management and board

Participate in discussions with the board and senior management about **key decisions** such as strategic planning and capital and liquidity planning and provide input to the board on compensation

Provide input to board on **incentive compensation** plan design and effectiveness

## Senior Management

## Chief Risk Officer

**Guide IRM** to establish and monitor compliance with enterprise-wide risk limits, identify and aggregate the firm's risks, assess risk positions relative to parameters of the firm's risk tolerance

## Independent Risk Management

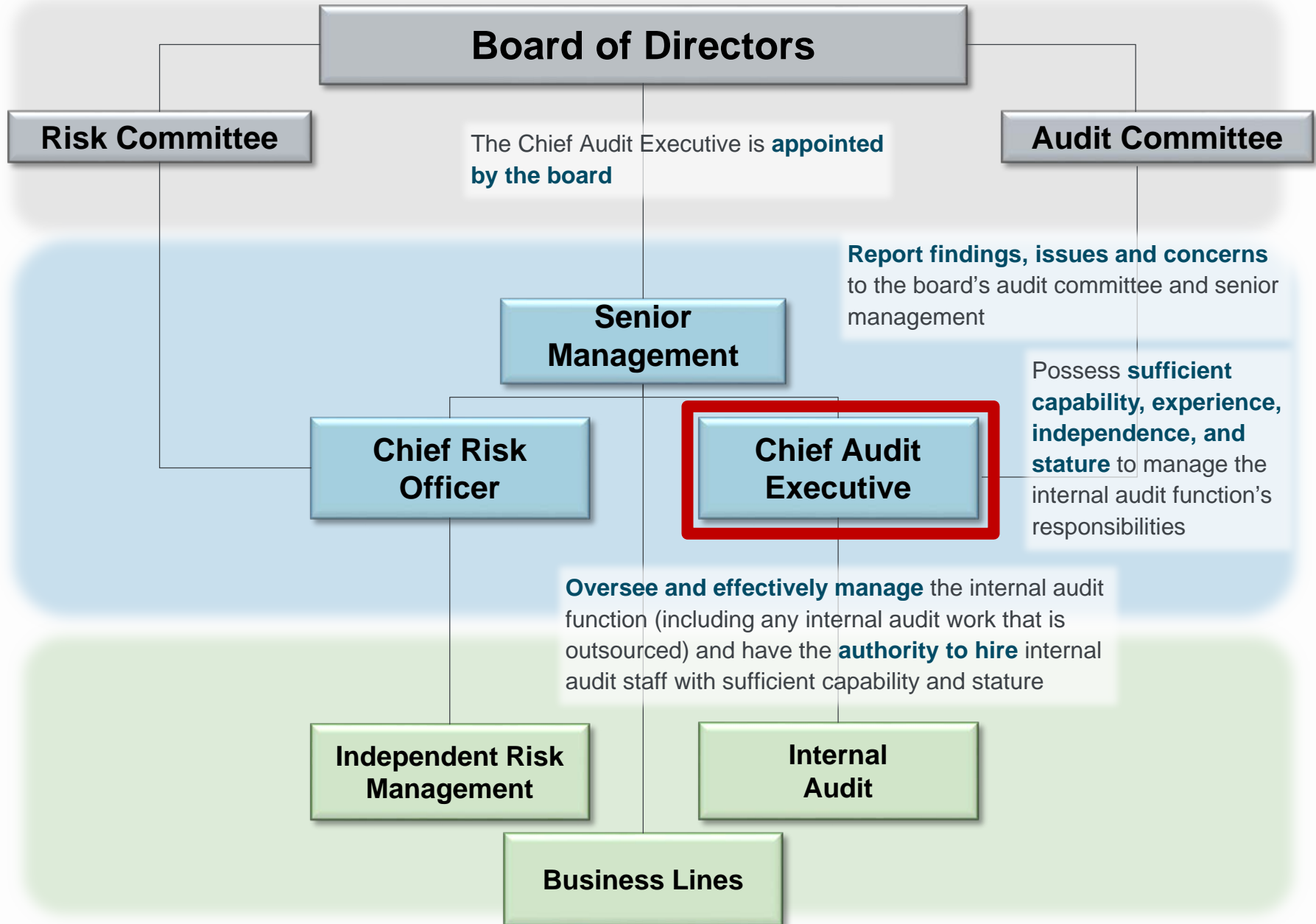
## Chief Audit Executive

## Internal Audit

## Business Lines

# Governance and Controls Component

SUPERVISORY EXPECTATIONS – GOVERNANCE, INDEPENDENCE AND STATURE - CAE





# Governance and Controls Component

## SUPERVISORY EXPECTATIONS – IRM

### Risk Tolerance

- Provide input into the firm’s risk tolerance and evaluate whether it:
  - Appropriately captures the firm’s material risks, including risks associated with revenue-generating activities, as well as other aspects of risks inherent to the business, such as compliance, information technology, and cybersecurity
  - Addresses risks under normal and stressed conditions and considers changes in the risk environment
  - Incorporates realistic risk and reward assumptions that, for example, do not overestimate expected returns from business activities or underestimate risks associated with business activities
  - Guides the firm’s risk-taking and risk mitigation activities
  - Aligns with the firm’s strategic plan and the corresponding business activities
  - Is consistent with the capacity of the risk management framework
- Determine whether the firm’s risk profile is consistent with its risk tolerance and assess whether the risk management framework has the capacity to manage the risks outlined in the risk tolerance
- Determine whether there are sufficient resources and infrastructure in the relevant areas of the firm to properly identify, manage, and report the risks associated with the business strategies outlined in the risk tolerance, including during stressful or unanticipated conditions

# Governance and Controls Component

## SUPERVISORY EXPECTATIONS – IRM

### Risk Limits

- Under the CRO's direction, establish enterprise-wide risk limits that are consistent with the firm's risk tolerance for the firm's full set of risks, including revenue-generating activities and those inherent to the business
- Create lower-level risk limits, such as for an individual business line, based on the enterprise-wide risk limits
- Monitor and update risk limits as appropriate, especially as the firm's risk tolerance, risk profile, or external conditions change
- Identify significant trends in risk levels to evaluate whether risk-taking and risk management practices are consistent with the firm's strategic objectives
- Escalate to senior management any material breaches of the firm's risk tolerance and enterprise-wide risk limits, as well as instances where IRM's conclusions differ from those of business lines

### Risk Limit Exceptions

The CRO or IRM should be involved in **any proposal to waive or make exceptions** to established risk limits, including on a temporary basis. They should provide an assessment of any such proposal and should escalate the proposal to the board of directors as appropriate.

# Governance and Controls Component

## SUPERVISORY EXPECTATIONS – IRM

### Risk limits should:

- Be assigned to specific risk types, business lines, legal entities, jurisdictions, geographic areas, concentrations, products or activities, commensurate with the firm's risk profile
- Be clear, relevant, and current
- Be quantitative and qualitative
- Include explicit thresholds that, if crossed, strictly prohibit the activity generating the risk
- Consider the range of possible external conditions facing the firm over a period of time
- Consider the aggregation and interaction of risks across the firm
- Be consistent with the firm's financial resources, such as available capital and liquidity, as well as with non-financial aspects, such as managerial, technological, and operational resources
- Reinforce compliance with laws and regulations, including those related to consumer protection, and consistency with supervisory expectations

### Quantitative risk limits

may be set relative to, for example:

- earnings;
- assets;
- liabilities;
- capital;
- liquidity; or
- other relevant benchmarks.

### Qualitative risk limits

are to be used as a proxy for risks or aspects of risks that are more difficult to quantify.

# Governance and Controls Component

## SUPERVISORY EXPECTATIONS – IRM

### Risk Identification and Measurement

- Identify and measure, on an ongoing basis, current and emerging risks within and across business lines and risk types, as well as any other relevant perspective
  - Identified risks should be regularly measured under both normal and stressful operating conditions, and considering the size and risk characteristics of the firm’s exposures and activities
  - Within each risk type, IRM should rely on a range of metrics and use appropriate measures
- Establish minimum internal standards, including quantitative and qualitative elements, for all of IRM’s risk identification and measurement practices to ensure consistent quality across different risks
- Ensure access to timely, reliable and comprehensive information about all risk-related exposures and activities, including emerging or potential risks
  - IRM should seek input across the firm in identifying risks and may use information collected from or used by business lines, but should not rely on business line information exclusively
  - IRM staff should also draw upon external information, such as peer data or market information, to supplement their assessments

# Governance and Controls Component

## SUPERVISORY EXPECTATIONS – IRM

### Risk Assessment

- Aggregate risks across the entire firm and assess those risks relative to the firm’s risk tolerance
  - Identify material or critical concentrations of risks and assess the likelihood and potential impact of those risks on the firm
  - Identify activities or exposures with related risk factors and assess their combined impact
- Assess risk information along different meaningful dimensions at a more granular level than firmwide – for example, by business line, geographic regions, obligors, counterparties, and products
- Conduct risk assessments using information from risk identification, measurement, and aggregation to determine the impact of risks on the firm and to inform senior management and the board about the suitability of risk positions relative to risk limits and the risk tolerance
  - Assess risks and risk drivers within and across business lines and risk types, as well as any other material perspectives
  - Analyze any assumptions related to risk diversification
  - Assess risk mitigation strategies, including the effectiveness of such mitigation in a range of circumstances, and recommend alternatives if concerns arise
- Identify information gaps, uncertainties, and limitations in risk assessments for senior management and, as appropriate, the board

# Governance and Controls Component

## SUPERVISORY EXPECTATIONS – IRM

### Risk Reporting

- Provide the board and senior management with risk reports that accurately and concisely convey relevant, material risk data and assessments in a timely manner
- Risk reporting should cover:
  - Current and emerging risks, including information on aggregate risks within and across business lines and risk types as well as by legal entity or jurisdiction and significant concentrations
  - Adherence to risk limits and risk concentrations
  - The firm’s ongoing strategic, capital, and liquidity planning processes
- Risk reporting should:
  - Enable prompt escalation and remediation of material problems
  - Enhance appropriate and timely responses to identified problems
  - Provide current and forward-looking perspectives
  - Support or influence strategic decision-making

The **frequency of risk reporting** will depend on the needs of the firm and the materiality of the issues.

Risk reporting must **adapt to market downturns** and stress events.

# Governance and Controls Component

## SUPERVISORY EXPECTATIONS – INTERNAL CONTROLS

- Responsibility for developing and maintaining effective internal controls belongs to senior management, IRM and business line management
  - A firm should appropriately assign management responsibilities for establishing and maintaining internal controls
- To foster an appropriate control culture within the firm, adequate control activities should be integrated into the daily functions of all relevant personnel
- A firm should have mechanisms to monitor and test internal controls and to identify and escalate issues that appear to compromise their effectiveness
- A firm should evaluate and communicate internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management
  - A firm should establish management information systems that track internal control weaknesses and escalate serious matters as appropriate

### Testing of Internal Controls

- The quality, reliability and effectiveness of internal controls should be regularly evaluated and tested
- The scope, frequency, and depth of testing should consider the complexity of the firm, the results of risk assessments, and the number and significance of the deficiencies identified during prior testing
- A firm should test and monitor internal controls using a risk-based approach, prioritizing efforts on controls in areas of highest risk and less effective controls

# Governance and Controls Component

## SUPERVISORY EXPECTATIONS – INTERNAL AUDIT

- The internal audit function should:
  - Examine, evaluate, and perform an independent assessment of the effectiveness of the firm’s risk management framework and internal control systems and
  - Report findings to senior management and the firm’s audit committee
- As part of evaluating a firm’s internal audit function under the LFI rating system, the Federal Reserve would assess the extent to which a firm complies with existing guidance on internal audit, which the Federal Reserve notes is not superseded by the Management Guidance
  - Existing guidance from the Federal Reserve on internal audit includes SR Letter 03-5 (outlining key components of an effective internal audit function) and SR Letter 13-1 (providing supplemental guidance that further addresses the characteristics, governance, and operational effectiveness of a firm’s internal audit function)



# 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>John Banes</b>           | <b>212 450 4116</b> | <a href="mailto:john.banes@davispolk.com"><u>john.banes@davispolk.com</u></a>               |
| <b>Luigi L. De Ghenghi</b>  | <b>212 450 4296</b> | <a href="mailto:luigi.deghenghi@davispolk.com"><u>luigi.deghenghi@davispolk.com</u></a>     |
| <b>Randall D. Guynn</b>     | <b>212 450 4239</b> | <a href="mailto:randall.guynn@davispolk.com"><u>randall.guynn@davispolk.com</u></a>         |
| <b>Jai R. Massari</b>       | <b>202 962 7062</b> | <a href="mailto:jai.massari@davispolk.com"><u>jai.massari@davispolk.com</u></a>             |
| <b>Annette L. Nazareth</b>  | <b>202 962 7075</b> | <a href="mailto:annette.nazareth@davispolk.com"><u>annette.nazareth@davispolk.com</u></a>   |
| <b>Gabriel D. Rosenberg</b> | <b>212 450 4537</b> | <a href="mailto:gabriel.rosenberg@davispolk.com"><u>gabriel.rosenberg@davispolk.com</u></a> |
| <b>Margaret E. Tahyar</b>   | <b>212 450 4379</b> | <a href="mailto:margaret.tahyar@davispolk.com"><u>margaret.tahyar@davispolk.com</u></a>     |
| <b>Leila Perkins</b>        | <b>212 450 3172</b> | <a href="mailto:leila.perkins@davispolk.com"><u>leila.perkins@davispolk.com</u></a>         |
| <b>Jennifer E. Kerlake</b>  | <b>212 450 6259</b> | <a href="mailto:jennifer.kerlake@davispolk.com"><u>jennifer.kerlake@davispolk.com</u></a>   |
| <b>Ryan Johansen</b>        | <b>212 450 3408</b> | <a href="mailto:ryan.johansen@davispolk.com"><u>ryan.johansen@davispolk.com</u></a>         |