

January 8, 2018

Federal Reserve Proposes Guidance to Clarify Supervisory Expectations Related to Risk Management for Large Financial Institutions

Proposed Guidance Presents Core Principles for Effective Senior Management, Management of Business Lines, and Independent Risk Management and Controls

SUMMARY AND OBSERVATIONS

On January 4, the Board of Governors of the Federal Reserve System (the *FRB*) issued a proposal for public comment that would set forth core principles of effective senior management, the management of business lines, and independent risk management (*IRM*) and controls for large financial institutions (*LFIs*). The proposed guidance, which was previewed by the FRB in two August 2017 proposals,¹ would apply to domestic bank holding companies and savings and loan holding companies with total consolidated assets of \$50 billion or more; the combined U.S. operations of foreign banking organizations (*FBOs*) with combined U.S. assets of \$50 billion or more; any state member bank subsidiaries of the foregoing; and systemically important nonbank financial companies designated by the Financial Stability Oversight Council for supervision by the FRB (*nonbank SIFIs*).² The proposal is intended to consolidate and clarify the FRB's existing expectations regarding risk management and delineate the roles and responsibilities for individuals and functions related to risk management. For those LFIs that would be subject to the previously proposed LFI rating system (bank holding companies, certain savings and loan holding companies and U.S. intermediate holding companies (*IHCs*) of *FBOs*), the proposed guidance would also inform the FRB's evaluation of each LFI's governance and controls for purposes of that rating system.

SULLIVAN & CROMWELL LLP

The proposal presents core risk management principles, as well as descriptions of the roles, responsibilities, and related expectations for covered individuals and functions, in the following areas:

- Effective senior management;
- Management of business lines;
- Roles and responsibilities of the chief risk officer (*CRO*) and chief audit executive (*CAE*);
- IRM;
- Internal controls; and
- Internal audit.

The proposal also addresses how certain aspects of the guidance would apply to the combined U.S. operations of covered FBOs, as well as how the guidance would inform supervisory evaluations of LFI that would not be subject to the proposed LFI rating system.

Notably, the proposal includes pervasive references to individuals or functions being expected to “ensure” various outcomes, including compliance with laws and regulations relating to consumer protection. The concept of “ensuring” outcomes appears to extend beyond the proposal’s definition of “internal controls,” which refers to “the policies, procedures, systems and processes *designed to provide reasonable assurance* regarding: the effectiveness and efficiency of operations; reliability of financial reporting (including risk reporting); compliance with laws and regulations (including those related to consumer protection); and safeguarding of assets and information.”³ In particular, although the focus on consumer compliance is understandable in view of recent developments, “ensuring” compliance appears unrealistic as a result of the highly complex and multiple sources of consumer compliance laws and regulations, and the subjective judgments that are often involved.

The references to management-level individuals or functions “ensuring” various outcomes distinguish this proposal from the FRB’s proposed guidance addressing supervisory expectations for boards of directors (the *BE guidance*), which generally does not include requirements or expectations that a board “ensure” a specific outcome, in contrast to much existing supervisory guidance on board responsibilities. Although the use of “ensure” in the current proposal likely reflects the FRB’s efforts to better distinguish the roles and responsibilities of senior management and the board,⁴ there are instances where characterizing management’s responsibility as “ensuring” various outcomes may not be a viable standard.

In addition, in discussing the relevant background of the proposed guidance, the FRB describes its consolidated supervisory framework for LFIs and explains that, drawing on the lessons from the 2007-2009 financial crisis, it “reevaluated its approach to supervision of LFIs, *including systemically important firms*.”⁵ The FRB also notes that it established the Large Institution Supervision Coordinating Committee (*LISCC*) “to coordinate its supervisory oversight for the systemically important firms *that pose the greatest risk to U.S. financial stability*.”⁶ Taken together, these statements (1) suggest that the FRB does not

SULLIVAN & CROMWELL LLP

regard all LFIs as systemically important and (2) reflect the FRB's differentiation among those LFIs that it regards as systemically important. The implications are notable, particularly in light of recent congressional efforts to revise post-crisis regulatory requirements, including increasing, from \$50 billion to \$250 billion, the asset threshold for automatic "SIFI" regulation of bank holding companies and FBOs under the Dodd-Frank Wall Street Reform and Consumer Protection Act.⁷

Other notable aspects of the proposal include the following:

- The branch operations of certain FBOs would be subject to the proposed guidance;
- The proposal employs a very broad definition of "business line" that could result in LFIs—and, in particular, LISCC firms—having numerous distinct "business lines" subject to the guidance;
- The proposal includes prescriptive and granular guidance on waivers, exceptions and breaches of risk limits; and
- The proposal represents another example of the FRB using notice and comment procedures to establish supervisory guidance.

Comments on the proposal are due by March 15, 2018.

BACKGROUND

The FRB notes that the proposal is part of a broader initiative to develop a supervisory rating system and related supervisory guidance that would align with its consolidated supervisory framework for LFIs. As part of that initiative, the FRB previously released two related proposals: a new rating system for LFIs (*proposed LFI rating system*) and the BE guidance. This proposal and the BE guidance together set forth supervisory expectations relevant to the assessment of the "governance and controls" component of the proposed LFI rating system.⁸

In the event that the proposed LFI rating system is finalized before this proposal, the FRB indicates that it would use existing supervisory guidance to inform its evaluation of governance and controls for purposes of that rating system. For firms that would be subject to this guidance but not the proposed LFI rating system, this guidance would inform the FRB's evaluation of those firms' safety and soundness and risk management practices. Firms that would be subject to this guidance but not the proposed LFI rating system are insurance or commercial savings and loan holding companies with total consolidated assets of \$50 billion or more, the combined U.S. operations of FBOs with \$50 billion or more of combined U.S. assets, state member bank subsidiaries of firms subject to the guidance, and nonbank SIFIs.⁹

The proposal for the LFI rating system included a summary of expectations for management of business lines and independent risk management and controls. The current proposal is generally consistent with that summary, with two distinctions. First, this proposal uses different terminology to identify the business lines to which the guidance would apply, eliminating the use of the term "core business lines." The FRB notes that this change does not affect the substance of the FRB's expectations. Second, this proposal

SULLIVAN & CROMWELL LLP

would apply to the combined U.S. operations of FBOs with combined U.S. assets of \$50 billion or more, including branch and subsidiary operations. The FRB's earlier summary of risk management expectations noted that the expectations would apply only to domestic LFIs, but that adjustments may be made to apply the guidance to the U.S. operations of FBOs before issuance for comment.

DISCUSSION

The proposal is intended to consolidate and clarify the FRB's existing supervisory expectations regarding risk management, as well as to delineate the roles and responsibilities for individuals and functions related to risk management. The delineation of roles and responsibilities is intended to enable the FRB to provide firms "more specific and consistent" supervisory feedback.

The FRB describes the proposal as complementing the BE guidance by (1) aligning the attributes of senior management with those of an effective board of directors and (2) better distinguishing expectations for boards from those of senior management. The proposal, for example, notes that a board sets the firm's strategy and risk tolerance and that senior management implements the strategy and risk tolerance approved by the board.

The proposal has three parts: (1) core principles of effective senior management; (2) core principles of the management of business lines; and (3) core principles of IRM and controls. The proposal also discusses specifically the applicability of the guidance to FBOs.

Reflecting a recent focus of the FRB and other financial services regulators on consumer protection, "ensuring" compliance with laws and regulations relating to consumer protection is an expectation noted throughout the proposal.

A. APPLICATION OF GUIDANCE TO FOREIGN BANKING ORGANIZATIONS

In addition to large domestic organizations, the proposal would apply to the combined U.S. operations, including branch and subsidiary operations, of FBOs with combined U.S. assets (including branch and subsidiary assets) of \$50 billion or more. The proposal states that the FRB's expectations for governance of the combined U.S. operations of FBOs are generally consistent with its expectations for governance of large domestic firms, while acknowledging that certain elements of an FBO's governance framework may be located outside the United States. Accordingly, the proposal highlights certain aspects of the guidance that might involve non-U.S. functions or individuals at FBOs and presents the FRB's expectations that senior management of an FBO should be informed of the risks of the FBO's U.S. operations and that information regarding those risks should be communicated to the FBO's global management.

The proposed LFI rating system would apply only to IHCs established by FBOs pursuant to the FRB's Regulation YY. The proposal, in contrast, would apply its risk management expectations to branch operations of FBOs and, consequently, to a much larger group of FBOs, including those that have

SULLIVAN & CROMWELL LLP

combined U.S. assets of \$50 billion or more, but non-branch assets below the \$50 billion threshold that triggers the IHC requirement, and to a much larger proportion of the U.S. operations of many FBOs subject to the IHC requirement.

B. CORE PRINCIPLES OF EFFECTIVE SENIOR MANAGEMENT

The proposal presents a broad, principle-based approach to the role of senior management, defining senior management as those directly accountable to the board of directors for the sound and prudent day-to-day management of the firm¹⁰ and responsible for “ensuring” safety and soundness and compliance with internal policies and procedures, laws, and regulations, including those related to consumer protection. The proposal highlights two key responsibilities of senior management: overseeing the activities of the firm’s business lines (individually and collectively) and overseeing the firm’s IRM and controls. The proposal also discusses senior management’s specific responsibilities and the FRB’s expectations as to how those responsibilities should be carried out, frequently in a prescriptive and granular manner.¹¹ The responsibilities of senior management include:

- Implementing the firm’s strategy and risk tolerance, as approved by the board; “ensuring” 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 identifying and escalating to the board instances where there is a risk that the firm’s activities collectively may deviate from the firm’s strategy and risk tolerance;
- Maintaining and implementing an effective risk management framework and “ensuring” that the firm appropriately manages risk consistent with its strategy and risk tolerance;
- Promoting and enforcing prudent risk-taking behaviors and business practices, including through the firm’s compensation and performance management programs;
- “Ensuring” effective communication and information sharing across the entire firm;
- Overseeing the firm’s day-to-day operations with robust mechanisms in place to allow decisions to be based on a full understanding of the firm’s risks and activities;
- Providing timely, useful, and accurate information to the board and being responsive to direction from the board and to the board’s needs for information; and
- “Ensuring” resolution of risk management issues (including those identified by the firm and in the context of outstanding supervisory matters), escalating issues to the board and communicating issues internally when appropriate.

The proposal addresses how certain of these expectations would apply to an FBO’s combined U.S. operations, including by noting that the risk tolerance for the combined U.S. operations may be developed separately for the IHC and branch operations, respectively, and that the strategy for the combined U.S. operations may refer to the manner in which the U.S. operations support the global strategy.

C. CORE PRINCIPLES FOR THE MANAGEMENT OF BUSINESS LINES

The proposal sets forth five core principles applicable to the management of business lines and critical operations.¹² A “business line” is very broadly defined as a unit or function, including associated

SULLIVAN & CROMWELL LLP

operations and support, that provides related products or services to meet the firm's business needs and those of its customers. The preamble notes that the definition would include units such as a firm's corporate treasury and IT support. "Critical operations" are those operations which, if they were to fail or discontinue, would pose a threat, in the view of the firm or the FRB, to the financial stability of the United States. "Business line management" consists of those who are responsible for the prudent day-to-day management of a business line and who report directly to senior management.

For an LFI that is an LISCC firm, the principles set forth in the proposal would apply to all of the firm's business lines due to the firm's size, risk profile, and systemic importance. For an LFI that is not an LISCC firm, the principles would apply to any business line in which a significant control disruption, failure, or loss event could result in a material loss of revenue, profit, or franchise value, or result in significant consumer harm. The proposal notes that LFI business lines not covered by the proposed guidance would be expected to maintain appropriate risk management practices to "ensure" the firm's safety and soundness.

The core principles cover five aspects of business line management: (1) implementation and execution of strategy and risk tolerance; (2) risk identification and risk management; (3) resources and infrastructure; (4) business controls; and (5) accountability. Specifically, business line management should:

- Execute business line activities consistent with the firm's strategy and risk tolerance;
- Identify, measure, and manage the risks associated with the business activities under a broad range of conditions, incorporating input from IRM;
- Provide a business line with the resources and infrastructure sufficient to manage the business line'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; and
- "Ensure" that the internal control system is effective for the business line operations.

Business line management and staff should also be accountable for operating within established policies and guidelines, and acting in accordance with applicable laws, regulations and supervisory guidance, including those related to consumer protection.

The proposal does not establish specific expectations regarding a firm's organizational structure, noting that business line management may also serve as senior management. If business line management is not part of senior management, business line management is responsible for fully engaging senior management so that members of senior management can effectively carry out their responsibilities.

The proposal notes that, for an FBO, a business line in the United States may be part of a larger global business line and, under these circumstances, the proposed guidance would apply only to that portion of the business conducted in the United States. Business line management of an FBO's U.S. operations is expected both to "ensure" that business line risks are captured comprehensively with consideration given

SULLIVAN & CROMWELL LLP

to risks outside of the United States that may impact the FBO's U.S. operations and to sufficiently inform and escalate to global management issues relating to U.S. business lines.

D. CORE PRINCIPLES OF INDEPENDENT RISK MANAGEMENT AND CONTROLS

The proposal identifies core principles in the following three areas: (1) IRM, which should provide an objective, critical assessment of risks and evaluate whether a firm remains aligned with its stated risk tolerance; (2) a system of internal control, which should guide practices, provide appropriate checks and balances and confirm quality of operations; and (3) internal audit, which should provide independent assessments of the effectiveness of the risk management framework and the system of internal control. The proposal also sets forth the specific roles and responsibilities of the CRO and CAE.

1. Governance, Independence and Stature

The proposal outlines principles relating to the roles and responsibilities of the CRO and CAE, respectively:

- The CRO should establish and maintain IRM that is appropriate for the size, complexity, and risk profile of the firm; and
- The CAE should have clear roles and responsibilities to establish and maintain an internal audit function that is appropriate for the size, complexity and risk profile of the firm.

In describing the role and responsibilities of the CRO, the FRB briefly summarizes the applicable requirements contained in Regulation YY.¹³ The FRB also provides additional, specific responsibilities of the CRO, including those relating to the CRO's oversight and support of the independence of IRM, the CRO's communications with senior management and the board (including informing the board of any concerns relating to the CRO's stature,¹⁴ independence, or authority) and escalation of issues to senior management and the board when activities or practices at the firm-wide, risk-specific, and business-line levels do not align with the firm's overall risk tolerance.

The CAE should be appointed by the board, and, consistent with prior FRB guidance, have sufficient capability, experience, independence, and stature to manage the internal audit function's responsibilities consistent with the size and complexity of the firm.¹⁵ Although the proposal describes certain responsibilities of the CAE at a high level, including overseeing outsourcing of internal audit work and hiring of internal audit staff, it does not provide the same level of detail as in the discussion of the CRO's responsibilities, consistent with the FRB's statement in the preamble that the proposal would not expand upon supervisory expectations for internal audit.

2. Independent Risk Management

The proposal provides that "independent risk management" consists of a range of risk management functions, noting, as an example, the function that establishes a firm-wide compliance risk management program. The proposal presents three categories of principles for IRM: (1) risk tolerance and limits; (2)

SULLIVAN & CROMWELL LLP

risk identification, measurement, and assessment; and (3) risk reporting. The proposed guidance builds upon the framework set forth in Regulation YY, which requires covered firms to have an independent risk management function.¹⁶

The FRB's expectations are that IRM should:

- Evaluate whether the firm's risk tolerance appropriately captures the firm's material risks and confirm that the risk tolerance is consistent with the capacity of the risk management framework;
- Establish enterprise-wide risk limits consistent with the firm's risk tolerance and monitor adherence to such limits;
- Identify and measure the firm's risks;
- Aggregate risks and provide an independent assessment of the firm's risk profile; and
- Provide the board and senior management with risk reports that accurately and concisely convey relevant, material risk data and assessments in a timely manner.

Although IRM is expected to evaluate the firm's risk tolerance, the proposal notes that the process of developing and updating a firm's risk tolerance is iterative, with multiple parties providing input on a continual basis. With regard to enterprise-wide risk limits, which IRM is expected to establish under the direction of the CRO, the proposal notes that business line management may develop its own limits for internal business line use and may provide input into the risk limit-setting process defined by IRM. However, the internal limits of a business line should not be less stringent than the limits set by IRM.

The core principles of both management of business lines and IRM contain prescriptive and granular guidance on waivers, exceptions, and breaches of risk limits. For example, business line management should consult with senior management before allowing *any* exceptions to risk limits and should evaluate breaches of risk limits to determine whether a breach was caused by a weakness in the business line's monitoring or limits framework and take appropriate remedial action. Moreover, risk limits should include explicit thresholds that, if crossed, strictly prohibit the activity generating the risk. IRM should escalate to senior management any material breaches of the firm's enterprise-wide risk limits and risk tolerance, as well as instances in which IRM's and a business line's conclusions differ.

3. Internal Controls

The proposal provides that internal controls cover a wide range of activities and processes and describes a number of systems, policies, and procedures.¹⁷ The FRB notes that the proposed guidance would expand upon the expectations for internal controls described in SR letter 12-17.

The proposal identifies two principles for internal controls:

- A firm should identify its system of internal control and demonstrate that it is commensurate with the firm's size, scope of operations, activities, risk profile, strategy, and risk tolerance, and that it is consistent with all applicable laws and regulations, including those related to consumer protection; and

SULLIVAN & CROMWELL LLP

- A firm should regularly evaluate and test the effectiveness of internal controls, and monitor their functioning so that deficiencies are identified and communicated in a timely manner.

The proposal provides that developing and maintaining effective internal controls is the responsibility of several parties, including business line management, and that internal controls should be examined, evaluated, and assessed by internal audit.

4. Internal Audit

The proposal would not expand upon the FRB's existing supervisory guidance for internal audit, which is described in SR letter 03-5 and SR letter 13-1/CA letter 13-1. The proposal describes the FRB's expectations regarding internal audit in accordance with the following principle:

- The internal audit function should examine, evaluate, and perform independent assessments of the firm's risk management and internal control systems and report findings to senior management and the firm's audit committee.

E. REQUEST FOR COMMENTS

The FRB requests comments on all aspects of the proposal, with comments due by March 15, 2018. The FRB is soliciting specific feedback on the following questions:

- What considerations beyond those outlined in the proposal should be considered in the FRB's assessment of whether an LFI has sound governance and controls such that the firm has sufficient financial and operational strength and resilience to maintain safe and sound operations?
- How could the relative roles and responsibilities of the board of directors set forth in the proposed BE guidance and the relative roles and responsibilities of senior management, business line management, and IRM set forth in this proposal be clarified?
- What, if any, aspects of the structure and coverage of IRM and controls should be addressed more specifically by the guidance?
- The proposal tailors expectations for FBOs, recognizing that the U.S. operations are part of a larger organization. How could this tailoring be improved?
- In what ways, if any, does the guidance diverge from industry practice? How could the guidance better reflect industry practice while facilitating effective risk management and controls? Are there any existing standards for internal control frameworks to which the guidance should follow more closely?
- Other supervisory communications have used the term "risk appetite" instead of risk tolerance. Are the terms "risk appetite" and "risk tolerance" used interchangeably within the industry, and what confusion, if any, is created by the terminology used in this guidance?
- The proposal would adopt different terminology than is used in the proposed LFI rating system, and the FRB expects to align the terminology so the element in the governance and controls component would change from "management of core business lines" to "management of business lines." Does this proposal clearly explain this expected change? Do commenters anticipate any impact from this change?

* * *

Copyright © Sullivan & Cromwell LLP 2018

ENDNOTES

- ¹ For a discussion of the FRB's prior proposals, for a new LFI rating system and revised supervisory expectations for banking organization boards of directors, respectively, see our memoranda to clients, "Federal Reserve Proposes New Rating System: Federal Reserve Proposes to Establish a New Rating System for the Supervision of Large Financial Institutions Designed to Align with the Supervisory Program for Those Institutions and to Enhance the Clarity and Consistency of Supervisory Assessments" (August 7, 2017), *available at* https://sullcrom.com/siteFiles/publications/SC_Publication_Federal_Reserve_Proposes_New_Rating_System.pdf; "Federal Reserve Proposes to Refocus Expectations for Banking Organization Directors on Core Responsibilities: Proposal Recognizes the Distinct Role of the Board as Compared to Management and the Adverse Impact of Unduly Extensive Requirements on the Board's Attention and Effectiveness" (August 7, 2017), *available at* https://sullcrom.com/siteFiles/publications/SC_Publication_Federal_Reserve_Proposes_to_Refocus_Expectations_for_Banking_Organization_Directors_on_Core_Responsibilities.pdf.
- ² Although these principles do not apply to non-LFIs, they are likely to inform supervisory evaluations of those firms.
- ³ Proposal, at 22 (emphasis added). The term "internal controls" is defined in a footnote accompanying a sentence noting the FRB's expectation that senior management "is responsible for developing and maintaining the firm's policies and procedures and system of internal control, commensurate with the firm's size, scope of operations, activities, and risk profile, *to ensure compliance with laws and regulations*, including those related to consumer protection, and consistency with supervisory expectations." (emphasis added).
- ⁴ Indeed, the FRB notes the complementary relationship between the current proposal and the BE guidance and that "the proposed guidance would better distinguish the supervisory expectations for boards from those of senior management." Proposal, at 7.
- ⁵ Proposal, at 3 (emphasis added).
- ⁶ *Id.* (emphasis added). The FRB's LISCC framework is designed to materially increase the financial and operational resiliency of systemically important financial institutions to reduce the probability of, and cost associated with, their material financial distress or failure. Firms subject to the LISCC framework currently include certain large bank holding companies, the U.S. operations of certain foreign banking organizations, and a nonbank SIFI. See <https://www.federalreserve.gov/bankinforeg/large-institution-supervision.htm>.
- ⁷ For a discussion of the "Economic Growth, Regulatory Relief, and Consumer Protection Act" recently approved by the U.S. Senate Banking Committee, see our memorandum to clients, "Financial Services Regulatory Reform Legislation: Senate Panel Approves Bipartisan Regulatory Reform Bill" (December 7, 2017), *available at* https://www.sullcrom.com/siteFiles/Publications/SC_Publication_Financial_Services_Regulatory_Reform_Legislation_12_07_2017.pdf.
- ⁸ For domestic bank holding companies subject to the LISCC framework, the "governance and controls" component would also include an evaluation of the effectiveness of their recovery planning, focusing on the extent to which their recovery planning processes effectively identify options that provide a reasonable chance of the firms being able to remedy financial weakness and restore market confidence without extraordinary official sector support. The FRB's supervisory guidance on recovery planning for those firms is set forth in Supervision and Regulation (SR) Letter 14-8.
- ⁹ The proposed LFI rating system would apply to domestic bank holding companies with total consolidated assets of \$50 billion or more; all non-insurance, non-commercial savings and loan holding companies with total consolidated assets of \$50 billion or more; and all IHCs.

ENDNOTES (CONTINUED)

- ¹⁰ The proposal provides that, for an FBO, “senior management” can refer to individuals located inside or outside the United States who are accountable to the IHC board, U.S. risk committee, or global board of directors with respect to the U.S. operations.
- ¹¹ The proposal’s presentation of a principles-based view that is supplemented with granular requirements and expectations parallels the structure of the BE guidance. Notably, a number of expectations for effective senior management provided in the proposal mirror expectations for effective boards of directors provided in the BE guidance. In particular:
- The proposal provides, “Senior management is responsible for implementing the firm’s strategy and risk tolerance approved by the board.” The BE guidance provides, “An effective board of directors guides the development of and approves the firm’s strategy and sets the types and levels of risk it is willing to take.”
 - The proposal provides, “Senior management is responsible for providing timely, useful, and accurate information to the board. Senior management should also be responsive to direction from the board and to the board’s informational needs.” The BE guidance provides, “[A]n effective board directs 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.”
 - The proposal provides, “Senior management should regularly report 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), and the outcomes of risk reviews which may result in remedial actions.” The BE guidance provides, “Boards of directors would remain responsible for holding senior management accountable for remediating supervisory findings.”
 - The proposal provides, “The CRO should inform the board if his or her stature, independence, or authority is not sufficient to provide objective and independent assessments of the firm’s risks, risk management activities, and system of internal control... A firm should have a CAE, appointed by the board, with sufficient capability, experience, independence and stature to manage the internal audit function’s responsibilities appropriate to the size and complexity of the firm.” The BE guidance provides, “An effective risk committee supports the stature and independence of the independent risk management function, including compliance, by communicating directly with the CRO on material risk management issues... An effective audit committee supports the stature and independence of internal audit by meeting directly with the CAE regarding the internal audit function, organizational concerns, and industry concerns.”
- ¹² The FRB notes in the preamble to the proposal that it would not expect to examine all of a firm’s covered business lines during a single year. Instead, the FRB would use a risk-based approach to determine which business lines of a firm to examine or review during the year. In determining which business lines to review in an upcoming examination cycle, the FRB would consider factors related to the potential for weaknesses in a firm’s governance and controls.
- ¹³ See 12 CFR 252.33; 12 CFR 252.155.
- ¹⁴ “Stature” is defined in the proposal to refer 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.
- ¹⁵ See SR letter 13-1/CA letter 13-1, “Supplemental Policy Statement on the Internal Audit Function and Its Outsourcing.”
- ¹⁶ See 12 CFR 252.33(a)(2)(ii)(C); 12 CFR 252.155(a)(2)(ii)(C).

ENDNOTES (CONTINUED)

- ¹⁷ In addition to listing specific examples of internal controls, the proposal cites to SR letter 03-5, “Amended Interagency Guidance on the Internal Audit Function and Its Outsourcing” as a relevant source.

SULLIVAN & CROMWELL LLP

ABOUT SULLIVAN & CROMWELL LLP

Sullivan & Cromwell LLP is a global law firm that advises on major domestic and cross-border M&A, finance, corporate and real estate transactions, significant litigation and corporate investigations, and complex restructuring, regulatory, tax and estate planning matters. Founded in 1879, Sullivan & Cromwell LLP has more than 875 lawyers on four continents, with four offices in the United States, including its headquarters in New York, four offices in Europe, two in Australia and three in Asia.

CONTACTING SULLIVAN & CROMWELL LLP

This publication is provided by Sullivan & Cromwell LLP as a service to clients and colleagues. The information contained in this publication should not be construed as legal advice. Questions regarding the matters discussed in this publication may be directed to any of our lawyers listed below, or to any other Sullivan & Cromwell LLP lawyer with whom you have consulted in the past on similar matters. If you have not received this publication directly from us, you may obtain a copy of any past or future publications by sending an email to SCPublications@sullcrom.com.

CONTACTS

New York

Thomas C. Baxter Jr.	+1-212-558-4324	baxtert@sullcrom.com
Jason J. Cabral	+1-212-558-7370	cabralj@sullcrom.com
Whitney A. Chatterjee	+1-212-558-4883	chatterjeew@sullcrom.com
H. Rodgin Cohen	+1-212-558-3534	cohenhr@sullcrom.com
Elizabeth T. Davy	+1-212-558-7257	davye@sullcrom.com
Mitchell S. Eitel	+1-212-558-4960	eitelm@sullcrom.com
Michael T. Escue	+1-212-558-3721	escuem@sullcrom.com
Jared M. Fishman	+1-212-558-1689	fishmanj@sullcrom.com
C. Andrew Gerlach	+1-212-558-4789	gerlacha@sullcrom.com
Wendy M. Goldberg	+1-212-558-7915	goldbergw@sullcrom.com
Charles C. Gray	+1-212-558-4410	grayc@sullcrom.com
Shari D. Leventhal	+1-212-558-4354	leventhals@sullcrom.com
Erik D. Lindauer	+1-212-558-3548	lindauere@sullcrom.com
Mark J. Menting	+1-212-558-4859	mentingm@sullcrom.com
Camille L. Orme	+1-212-558-3373	ormec@sullcrom.com
Stephen M. Salley	+1-212-558-4998	salleys@sullcrom.com
Rebecca J. Simmons	+1-212-558-3175	simmonsr@sullcrom.com
William D. Torchiana	+1-212-558-4056	torchianaw@sullcrom.com
Donald J. Toumey	+1-212-558-4077	toumeyd@sullcrom.com
Marc Trevino	+1-212-558-4239	trevinom@sullcrom.com

SULLIVAN & CROMWELL LLP

Benjamin H. Weiner	+1-212-558-7861	weinerb@sullcrom.com
Mark J. Welshimer	+1-212-558-3669	welshimerm@sullcrom.com
Michael M. Wiseman	+1-212-558-3846	wisemanm@sullcrom.com
<hr/> Washington, D.C.		
Eric J. Kadel, Jr.	+1-202-956-7640	kadelej@sullcrom.com
William F. Kroener III	+1-202-956-7095	kroenerw@sullcrom.com
Stephen H. Meyer	+1-202-956-7605	meyerst@sullcrom.com
Jennifer L. Sutton	+1-202-956-7060	suttonj@sullcrom.com
Andrea R. Tokheim	+1-202-956-7015	tokheima@sullcrom.com
Samuel R. Woodall III	+1-202-956-7584	woodalls@sullcrom.com
<hr/> Los Angeles		
Patrick S. Brown	+1-310-712-6603	brownp@sullcrom.com
William F. Kroener III	+1-310-712-6696	kroenerw@sullcrom.com
<hr/> Paris		
William D. Torchiana	+33-1-7304-5890	torchianaw@sullcrom.com
<hr/> Melbourne		
Robert Chu	+61-3-9635-1506	chur@sullcrom.com
<hr/> Tokyo		
Keiji Hatano	+81-3-3213-6171	hatanok@sullcrom.com