FEDERAL RESERVE SYSTEM

Docket No. OP- 1594

AGENCY: Board of Governors of the Federal Reserve System (Board).

ACTION: Proposed supervisory guidance.

SUMMARY: The Board is seeking comment on proposed guidance describing core principles of effective senior management, the management of business lines, and independent risk management and controls for large financial institutions. The proposal would apply to domestic bank holding companies with total consolidated assets of $50 billion or more; savings and loan holding companies with total consolidated assets of $50 billion or more; the combined U.S. operations of foreign banking organizations 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 Board.

DATES: Comments must be received no later than March 15, 2018.

ADDRESSES: Interested parties are invited to submit written comments by following the instructions for submitting comments at

http://www.federalreserve.gov/generalinfo/foia/ProposedRegs.cfm.

• *Federal eRulemaking Portal: http://www.regulations.gov.* Follow the instructions for submitting comments.

• *Email: regs.comments@federalreserve.gov.* Include the docket number in the subject line of the message.

• *Fax:* (202) 452-3819 or (202) 452-3102.

• *Mail:* Address to Ann E. Misback, Secretary, Board of Governors of the Federal Reserve System, 20th Street and Constitution Avenue NW, Washington, DC 20551.

All public comments will be made available on the Board's website at *http://www.federalreserve.gov/generalinfo/foia/ProposedRegs.cfm* as submitted, unless modified for technical reasons. Accordingly, comments will not be edited to remove any identifying or contact information. Public comments may also be viewed electronically or in paper in Room 3515, 1801 K Street NW (between 18th and 19th Street NW), Washington, DC 20006 between 9:00 a.m. and 5:00 p.m. on weekdays.

FOR FURTHER INFORMATION CONTACT: Michael Hsu, Associate Director, (202) 912-4330, Richard Naylor, Associate Director, (202) 728-5854, Vaishali Sack, Manager, (202) 452-5221, April Snyder, Manager, (202) 452-3099, David Palmer, Senior Supervisory Financial Analyst, (202) 452-2904, Jennifer Su, Senior Supervisory Financial Analyst, (202) 475-6348, Christine Graham, Senior Supervisory Financial Analyst, (202) 452-3005, Division of Supervision and Regulation; Laurie Schaffer, Associate General Counsel, (202) 452-2272, Benjamin W. McDonough, Assistant General Counsel, (202) 452-2036, Scott Tkacz, Senior Counsel, (202) 452-2744, Keisha Patrick, Senior Counsel, (202) 452-3559, or Christopher Callanan, Senior Attorney, (202) 452-3594, Legal Division, Board of Governors of the Federal Reserve System, 20th and C Streets, NW, Washington, DC 20551. For the hearing impaired only, Telecommunications Device for the Deaf (TDD) users may contact (202) 263-4869.

SUPPLEMENTARY INFORMATION:

Table of Contents

I. Background

The Board invites comment on proposed guidance setting forth core principles of effective senior management, the management of business lines, and independent risk management ("IRM") and controls for large financial institutions ("LFIs"). This proposal is part of a broader initiative by the Federal Reserve to develop a supervisory rating system and related supervisory guidance that would align with its consolidated supervisory framework for LFIs. Drawing on lessons from the 2007-2009 financial crisis, the Federal Reserve reevaluated its approach to supervision of LFIs, including systemically important firms. In 2010, the Federal Reserve 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.[1] In 2012, the Federal Reserve implemented a new consolidated supervisory program for LFIs ("LFI supervision framework") described in SR letter 12-17.[2] The

[1] Presently, the LISCC portfolio consists of eight domestic bank holding companies, four foreign banking organizations, and one nonbank financial company designated by the Financial Stability Oversight Council ("FSOC") for supervision by the Federal Reserve. The domestic bank holding companies are: (1) Bank of America Corporation; (2) Bank of New York Mellon Corporation; (3) Citigroup Inc.; (4) Goldman Sachs Group, Inc.; (5) JP Morgan Chase & Co.; (6) Morgan Stanley; (7) State Street Corporation; and (8) Wells Fargo & Company. The foreign banking organizations are: (1) Barclays PLC; (2) Credit Suisse Group AG; (3) Deutsche Bank AG; and (4) UBS AG. The nonbank financial company is Prudential Financial, Inc. The list of firms included in the LISCC supervisory program is available at https://www.federalreserve.gov/bankinforeg/large-institution-supervision.htm. Hereinafter in this preamble, these firms may be referred to as "LISCC firms."

[2] See SR letter 12-17/CA letter 12-14, "Consolidated Supervision Framework for Large Financial Institutions," (referred to as "SR letter 12-17" in this preamble).

LFI supervision framework is focused on four core areas—capital planning and positions, liquidity risk management and positions, governance and controls, and resolution planning.[3]

II. LFI Rating System and Board Effectiveness Proposals

In August 2017, the Board invited comment on two proposals that relate to this guidance, a new rating system for LFIs ("proposed LFI rating system")[4] and proposed guidance addressing supervisory expectations for boards of directors ("BE proposal").[5] On November 17, 2017, the Board extended the public comment period for the proposed LFI rating system and BE proposal until February 15, 2018, to give the public an opportunity to understand and comment on the proposed LFI rating system, the BE proposal, and this proposed guidance together.

The proposed LFI rating system would provide a supervisory evaluation of whether a firm possesses sufficient financial and operational strength and resilience to maintain safe and sound operations through a range of conditions. Consistent with the LFI supervision framework, the proposed LFI rating system would include assessments of a firm's capital, liquidity, and governance and controls. As discussed further below, the BE proposal and this proposal set forth supervisory expectations relevant to the assessment of a firm's governance and controls.

The governance and controls component would consist of three elements: (i) effectiveness of a firm's board of directors, (ii) management of business lines and

---

[3] The Board previously set forth expectations for resolution planning for domestic LISCC firms in SR letter 14-8, "Consolidated Recovery Planning for Certain Large Domestic Bank Holding Companies."

[4] 82 FR 39049 (August 17, 2017). The proposed LFI rating system would apply to all 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 U.S. intermediate holding companies of foreign banking organizations established pursuant to the Federal Reserve's Regulation YY.

[5] 82 FR 37219 (August 9, 2017).

independent risk management and controls, and (iii) recovery planning (for domestic LISCC firms only).

To facilitate comment on the proposed LFI rating system, the preamble to the proposed LFI rating system included a summary which previewed the proposed expectations included in this proposal. This proposal is generally consistent with that summary, with two exceptions. First, this proposal expands the scope of the guidance to foreign banking organizations.[6] Second, this proposal adopts slightly different terminology than is used in the proposed LFI rating system to describe expectations for the management of business lines. However, the change does not change the substance of those expectations described in the proposed LFI rating system.[7] The Board would expect to apply the terminology used in this guidance in any final LFI rating system; however, this change would not impact the supervisory assessment of a firm's management of business lines for purposes of the governance and controls component rating.

The BE proposal sets forth attributes of an effective board of directors. It is intended to better distinguish the supervisory expectations for boards from those of senior management and encourage boards to focus time and attention on their core responsibilities.[8] The expectations in

---

[6] The preamble to the proposed LFI rating system described the management of business lines and IRM and controls for domestic LFIs, and noted that adjustments to extend applicability of the guidance to the U.S. operations of FBOs may be made prior to issuing this guidance for public comment. This preamble highlights those adjustments.

[7] See discussion of this change in section VI.B of this preamble.

[8] "Board" or "board of directors" also refers to committees of the board of directors, as appropriate.

At this time, recovery planning expectations apply only to domestic bank holding companies in the LISCC portfolio. See SR letter 14-8, "Consolidated Recovery Planning for Certain Large Domestic Bank Holding Companies." Should the Federal Reserve expand the scope of recovery planning expectations to encompass additional firms, this rating will reflect such expectations for the broader set of firms.

the BE proposal would inform the Board's evaluation of the effectiveness of a firm's board of directors under the governance and control component of the proposed LFI rating system.

III. Implementation

The proposed LFI rating system would provide a supervisory evaluation of whether a firm possesses sufficient financial and operational strength and resilience to maintain safe and sound operations through a range of conditions. This proposed guidance builds upon the proposed LFI rating system framework by providing additional detail regarding supervisory expectations for a firm's management of business lines and independent risk management and controls. For firms that would be subject to the proposed LFI rating system, these expectations would help inform the Federal Reserve's overall supervisory evaluation, for purposes of the proposed LFI rating system, of each firm's governance and controls to support the firm's financial and operational strength and resilience, which would be reflected by the governance and controls component rating under the proposed LFI rating system.[9]

The Federal Reserve would not expect to examine all of a firm's business lines which are subject to this proposed guidance during a single year. Instead, consistent with its current supervisory practice, the Federal Reserve would use a risk-based approach to determine which business lines of a firm to examine or review during the year. In conducting its supervisory planning for an upcoming exam cycle, the Federal Reserve would consider factors related to the

[9] The Federal Reserve expects to finalize the proposed guidance for use in assigning initial ratings under the LFI rating system beginning in 2018. If the proposed LFI rating system were finalized before this proposed guidance, the Federal Reserve would use existing supervisory guidance to help inform its evaluation of each firm's governance and controls for purposes of the proposed LFI rating system, until such time that this proposed guidance is finalized.

For firms that would be subject to this proposed guidance but not subject to the proposed LFI rating system, this proposed guidance would help inform the Federal Reserve's evaluation of the firm's overall safety and soundness and the effectiveness of its risk management practices.

potential for weaknesses in a firm's governance and controls.[10] Such factors would include the size and complexity of the business line, recent supervisory experience, the relative growth and maturity of the business line, and significant changes to strategy, structure, or management since the last exam cycle. In order to minimize unnecessary duplication for firms subject to this guidance, the Federal Reserve would, to the extent possible, evaluate a firm's governance and controls in coordination with other relevant Federal and state agencies, particularly the primary regulators of the firm's insured depository institution subsidiaries.

IV. Objectives of the Proposed Guidance

The proposed guidance is intended to consolidate and clarify the Federal Reserve's existing supervisory expectations regarding risk management.[11] In addition, the proposed guidance is designed to delineate the roles and responsibilities for individuals and functions related to risk management. It would complement the BE proposal by aligning the attributes of senior management with those of an effective board of directors. For instance, the BE proposal provides that an effective board of directors sets the firm's strategy and risk tolerance, and this proposal contemplates that the firm's senior management implements the strategy and risk tolerance approved by the board. In this way, the proposed guidance would better distinguish the supervisory expectations for boards from those of senior management. The proposal also defines

[10] For supervisory planning purposes, the Federal Reserve may reevaluate at any time which areas of a firm to examine or review, as circumstances warrant.

[11] For firms subject to this proposed guidance, the proposed guidance would supersede SR letter 95-51, "Rating the Adequacy of Risk Management Processes and Internal Controls at State Member Banks and Bank Holding Companies." SR letter 95-51 was superseded by SR letter 16-11 for state member banks, bank holding companies, and savings and loan holding companies (including insurance and commercial savings and loan holding companies) with less than $50 billion in total consolidated assets, and FBOs with consolidated U.S. assets of less than $50 billion. See SR letter 16-11, "Supervisory Guidance for Assessing Risk Management at Supervised Institutions with Total Consolidated Assets Less than $50 Billion."

the roles and responsibilities for various individuals and functions within an organization that are accountable for risk management, including a firm's senior management, business line management, and independent risk management and audit functions. Delineating roles and responsibilities for risk management should enable the Federal Reserve to provide firms with more specific and consistent supervisory feedback.

V. Applicability

The proposed guidance would apply to domestic bank holding companies with total consolidated assets of $50 billion or more; 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 FSOC for supervision by the Board.[12]

For FBOs, the proposed guidance would apply to an FBO's combined U.S. operations, including branch and subsidiary operations. This scope would be consistent with certain requirements of the Board's Regulation YY, which requires, among other things, FBOs to establish a risk management framework that covers both the U.S. branch and U.S. non-branch subsidiary operations, establish a U.S. risk committee to oversee the risks of the combined U.S. operations, and employ a chief risk officer ("CRO") based in the United States.[13]

---

[12] As described in the proposed guidance, references to "firm" refer to all entities subject to this guidance, including the combined U.S. operations of an FBO, unless the context requires otherwise.

[13] 12 CFR 252.155. For an FBO, references to CRO mean the U.S. CRO. Unlike this proposal, the BE proposal would not apply to the U.S. operations of a foreign banking organization, due to concerns of extraterritoriality and differences in organizational structure and legal requirements in other jurisdictions. In the preamble to the BE proposal, the Board stated that it was considering applying that guidance to the boards of directors of U.S. intermediate holding companies, and sought comment on that proposed application.

Given that an FBO's combined U.S. operations are part of a larger global organization, the proposed guidance notes that certain elements of an FBO's governance framework may be located outside of the United States. In this event, the proposed guidance provides that these elements should enable effective governance and risk management by the U.S. senior management, the U.S. risk committee, and the intermediate holding company ("IHC") board (as applicable), and should facilitate U.S. supervisors' ability to assess the adequacy of governance and controls in the combined U.S. operations.

The proposed guidance also applies to nonbank financial companies supervised by the Board and insurance or commercial savings and loan holding companies with total consolidated assets of $50 billion or more. The concepts set forth in the proposed guidance relate to fundamental risk management practices that are applicable to all LFIs.

VI. Description of the Proposed Guidance

The proposed guidance is organized in 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.

A. Core Principles of Effective Senior Management

The proposed guidance sets forth core principles of effective senior management. Senior management is defined as the core group of individuals directly accountable to the board of directors for the sound and prudent day-to-day management of the firm. Under the board's oversight, a firm's senior management is responsible for managing the day-to-day operations of the firm and ensuring safety and soundness and compliance with laws and regulations, including those related to consumer protection, and internal policies and procedures. Two key responsibilities of senior management are overseeing the activities of the firm's business lines

(individually and collectively) and the firm's IRM and system of internal control. In addition to the general expectations regarding senior management, the IRM and controls section of the proposed guidance sets forth specific expectations for the CRO and chief audit executive ("CAE"), as these individuals have specific responsibilities related to IRM and internal audit, respectively.

The proposed guidance tailors the application of these expectations for an FBO, given that the combined U.S. operations are part of a larger global organization. For instance, the proposed guidance notes that the risk tolerance for the combined U.S. operations may be developed separately for the IHC and branch operations, respectively, and notes that the strategy for the combined U.S. operations may mean the manner in which the U.S. operations support the global strategy. The proposal also notes 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.[14]

B. Core Principles of the Management of Business Lines

The proposed guidance sets forth core principles of the management of business lines. Business line management is defined as the core group of individuals responsible for the prudent day-to-day management of the business line and who report directly to senior management.[15]

---

[14] To facilitate a full understanding by the FBO of risks presented by the U.S. operations, the proposed guidance states that senior management should fully understand U.S.-based risks and communicate information on those risks to global management so that U.S.-based risks are included in the aggregate risk assessment.

[15] The proposed guidance defines a business line as 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. This definition would include units such as Corporate Treasury and IT support. For an FBO, a business line would include all business lines that are present in the United States.

Business line management is expected to execute business line activities consistent with the firm's strategy and risk tolerance, identify and manage risk within the business line, provide sufficient resources and infrastructure to the business line, ensure the business line has the appropriate system of internal control, and ensure accountability for operating within established policies and guidelines and in accordance with laws and regulations, including those related to consumer protection.

For a LISCC firm, due to its size, risk profile, and systemic importance of operations, the core principles of the management of business lines would apply to all of the firm's business lines. For an LFI that is not a LISCC firm, the core principles of the management of business lines would apply to any business line where 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.[16] The proposed guidance uses slightly different terminology than the proposed LFI rating system to describe the core principles of the management of business lines. The proposed LFI rating system referred to these principles as relating to the "management of core business lines." For a LISCC firm, "core" business lines were defined to include all business lines, whereas for other LFIs, "core" business lines were defined to include any business line where a significant control disruption, failure, or loss event could result in a material loss of

[16] Any business line of an LFI that is not a LISCC firm which does not meet this definition (and thus would not be subject to the core principles of the management of business lines included in Part II of the proposed guidance) would be expected to maintain appropriate risk management practices to ensure the firm's safety and soundness. In addition, the supervisory expectations concerning effective senior management oversight and IRM and controls described in Parts I and III of the proposed guidance, respectively, would apply across the entire firm. For example, supervisory expectations regarding senior management's responsibility for maintaining and implementing an effective risk management framework and ensuring that the firm appropriately manages risk consistent with the firm's strategy and risk tolerance extends to its management of the firm as a whole, and not be limited to the individual business lines covered by Part II of the proposed guidance.

revenue, profit, or franchise value, or result in significant consumer harm. Although this proposal uses the term "management of business lines," the principles would apply to the same business lines that were identified as "core" in the proposed LFI rating system. The revised terminology is intended to simplify the guidance.

The proposed guidance does not include specific expectations regarding organizational structure at firms and states 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 senior management can effectively carry out their responsibilities.

For an FBO, the proposed guidance acknowledges that a business line in the United States may be part of a larger global business line and clarifies that the guidance applies only to that portion of the business conducted in the United States. The proposed guidance notes that business line management should ensure that business line risks are comprehensively captured, with consideration given to risks outside of the United States that may impact the FBO's U.S. operations.[17]

C. Core Principles of Independent Risk Management and Controls

The proposed guidance describes core principles of a firm's IRM and controls, which refers to a firm's independent risk management function, system of internal control, and internal audit function.[18] The proposal sets forth responsibilities of the CRO and CAE, the members of

[17] Conversely, to ensure that risks of the U.S. operations are appropriately communicated to global management, business line management would be expected to provide sufficient information to global management and escalate issues, as appropriate, to enable an understanding of U.S. risk.

[18] The proposed guidance defines the term "internal controls" as the policies, procedures, systems and processes designed to provide reasonable assurance regarding: the effectiveness and

senior management responsible for IRM and internal audit, respectively. As described in the proposed guidance, both the CRO and CAE should have clear roles and responsibilities to establish and maintain an IRM and internal audit function, respectively, that are appropriate for the size, complexity, and risk profile of the firm.

The proposed guidance describes expectations for a firm's IRM, which include evaluating the firm's risk tolerance; establishing enterprise-wide risk limits and monitoring adherence to those limits; identifying, measuring, and aggregating risks; providing an independent assessment of the firm's risk profile; and providing risk reports to the board and senior management. The proposed guidance builds upon the framework set forth in Regulation YY, which requires a firm to have an independent risk management function.[19]

While IRM would be expected to evaluate the firm's risk tolerance, the proposed guidance would not set the expectation that IRM would have sole responsibility for the risk tolerance. Depending on a firm's organizational structure, it may be appropriate for business line management to provide input into the risk tolerance or drive its development. The proposed guidance would assign responsibility for enterprise-wide risk limits to IRM, but acknowledge that business line management may develop its own limits for internal business line use and may provide input to 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 because the IRM limits should be the operative, formal, and binding limits across the firm.

---

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.

[19] 12 CFR 252.33, 252.155. See also SR letter 12-17.

For internal controls, the proposed guidance expands upon the expectation for internal controls described in SR letter 12-17. As described in the proposed guidance, a firm should identify its system of internal control and demonstrate that that system is commensurate with the firm's size, scope of operations, activities, risk profile, strategy, and risk tolerance; demonstrate that it is consistent with all applicable laws and regulations; regularly evaluate and test the effectiveness of internal controls; and monitor the functioning of controls so that deficiencies are identified and communicated in a timely manner. The proposed guidance provides that developing and maintaining effective internal controls is the responsibility of several parties, including business line management.

The strength of a firm's internal audit practices are an important consideration in the Federal Reserve's supervisory assessment of the effectiveness of the firm's governance and controls. This proposed guidance would not expand upon the Federal Reserve's expectations for internal audit; instead the proposed guidance references existing guidance.[20]

VII. Request for Comments

The Board invites comments on all aspects of the proposed guidance, including responses to the following questions:

1) What considerations beyond those outlined in this proposal should be considered in the Federal Reserve'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?

[20] The Federal Reserve issued guidance outlining the key components of an effective internal audit function in SR letter 03-5, "Amended Interagency Guidance on the Internal Audit Function and its Outsourcing," and followed that with supplemental guidance in SR letter 13-1/CA letter 13-1, "Supplemental Policy Statement on the Internal Audit Function and Its Outsourcing."

2) How could the roles and responsibilities between the board of directors set forth in the proposed board effectiveness guidance, and between the senior management, business line management, and IRM be clarified?

3) What, if any, aspects of the structure and coverage of IRM and controls should be addressed more specifically by the guidance?

4) The proposal tailors expectations for FBOs, recognizing that the U.S. operations are part of a larger organization. How could this tailoring be improved?

5) 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?

6) 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?

7) The proposal would adopt different terminology than is used in the proposed LFI rating system, and the Board 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?

Paperwork Reduction Act

In accordance with the Paperwork Reduction Act of 1995 (44 U.S.C. 3501-3521) ("PRA"), the Board may not conduct or sponsor, and a respondent is not required to respond to, an information collection unless it displays a currently valid Office of Management and Budget

("OMB") control number. The Board reviewed the proposed supervisory guidance under the authority delegated to the Board by OMB.

The proposed supervisory guidance contains a collection of information subject to the PRA. Recordkeeping requirements are found in the proposed guidance. Among expectations for business line management, the proposed guidance states that business line management should establish specific business and risk objectives for business lines, and establish policies and guidelines that delineate accountability within the business line. In addition, the proposed guidance sets expectations for a firm's IRM function, including related to the scope of a firm's risk limits and an expectation for written risk assessment that would be provided to the senior management and, as appropriate, the board. The proposed guidance also sets expectations for internal audit, including an expectation for an internal audit risk assessment and audit reports.

Comments are invited on:

a. Whether the collections of information are necessary for the proper performance of the Board's functions, including whether the information has practical utility;

b. The accuracy or the estimate of the burden of the information collections, including the validity of the methodology and assumptions used;

c. Ways to enhance the quality, utility, and clarity of the information to be collected;

d. Ways to minimize the burden of the information collections on respondents, including through the use of automated collection techniques or other forms of information technology; and

e. Estimates of capital or startup costs and costs of operation, maintenance, and purchase of services to provide information.

All comments will become a matter of public record. Comments on aspects of this notice that may affect reporting, recordkeeping, or disclosure requirements and burden estimates should be sent to: Secretary, Board of Governors of the Federal Reserve System, 20th and C Streets NW, Washington, DC 20551. A copy of the comments may also be submitted to the OMB desk officer by mail to U.S. Office of Management and Budget, 725 17th Street NW, #10235, Washington, DC 20503; facsimile to (202) 395-6974; or e-mail to oira_submission@omb.eop.gov, Attention, Federal Banking Agency Desk Officer.

Proposed Information Collection

Report title: Governance and Controls Guidance.

Agency form number: FR 4204.

OMB control number: 7100-NEW.

Frequency: Annual.

Respondents: Domestic bank and savings and loan holding companies with total consolidated assets of $50 billion or more, systemically important nonbank financial companies designated by FSOC for supervision by the Board, the U.S. operations of FBOs with combined U.S. assets of $50 billion or more, and state member bank subsidiaries of the foregoing.

Legal authorization and confidentiality: This information collection is voluntary. The Board has determined that the collection of information is authorized by section 5(c) of the Bank Holding Company Act (12 U.S.C. 1844(c)), section 10(b) of the Homeowners' Loan Act (12 U.S.C. 1467a(b)(4), section 113 of the Dodd-Frank Act (12 U.S.C. 5323). The information contained would be considered confidential pursuant to exemption 8 of the Freedom of Information Act (5 U.S.C. 552(b)(8)).

Estimated number of respondents: 56.

Estimated average hours per response: 3,872 hours initial setup, 560 hours for ongoing.

Estimated annual burden hours: 216,832 hours initial setup, 31,360 hours for ongoing.

Regulatory Flexibility Analysis

The Federal Reserve is providing an initial regulatory flexibility analysis with respect to this proposal. While the proposed guidance is not being adopted as a rule, the Federal Reserve has considered the potential impact of the proposal on small banking organizations using considerations that would apply if the Regulatory Flexibility Act, 5 U.S.C. 601 et. seq. ("RFA") were applicable. Based on the Board's analysis and for the reasons stated below, the Board believes that the proposed guidance will not have a significant economic impact on a substantial number of small entities.

Under regulations issued by the Small Business Administration, a small entity includes a depository institution, bank holding company, or savings and loan holding company with assets of $550 million or less ("small banking organizations"). As of June 1, 2017, there were approximately 3,539 small banking organizations. As described above, the proposed guidance would apply only to all bank holding companies with total consolidated assets of $50 billion or more; state member banks of such bank holding companies; all savings and loan holding companies with total consolidated assets of $50 billion or more; systemically important nonbank financial companies designated by FSOC for supervision by the Federal Reserve; and the U.S. operations of FBOs with combined U.S. assets of $50 billion or more. Small banking organizations would therefore not be subject to the proposed guidance. As a result, the proposed guidance should have any impact on small banking organizations. In light of the foregoing, the Board believes that the proposed guidance will not have a significant economic impact on small banking organizations supervised by the Board.

Text for the Proposed Supervisory Guidance on Management of Business Lines and Independent Risk Management and Controls for Large Financial Institutions

Introduction

Governance and controls involves (i) the oversight of a firm by its board of directors, (ii) management of business lines and independent risk management (IRM) and controls, and (iii) for domestic Large Institution Supervision Coordinating Committee (LISCC) firms only, recovery planning. This guidance sets forth the second part of the Federal Reserve's expectations for large financial institutions (LFIs or firms) – core principles of the management of business lines and IRM and controls. This guidance also builds upon supervisory guidance previously issued by the Federal Reserve.[21]

Guidance related to the first part of governance and controls, the oversight of a firm by its board of directors (BE Guidance), was released earlier.[22] It describes attributes of an effective board of directors and distinguishes a board's responsibilities from those of a firm's senior management.

Like the BE Guidance, the supervisory expectations described in this guidance regarding the management of business lines and IRM and controls would help inform the Federal Reserve's overall supervisory evaluation of a firm's governance and controls to support the firm's financial and operational strength and resilience. Among other factors, this evaluation would be an input to the governance and controls component rating under the proposed LFI rating system.[23]

I. Applicability

The guidance applies to domestic bank holding companies (BHCs) and domestic 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, and any state member bank subsidiaries of the foregoing. The guidance also applies to

---

[21] See SR letter 12-17 / CA letter 12-14, "Consolidated Supervision Framework for Large Financial Institutions." Other laws and regulations set forth requirements for corporate governance and risk management, including the risk and liquidity risk management requirements in Regulation YY (12 CFR part 252).

[22] See 82 FR 37219 (August 9, 2017) for the proposed Supervisory Guidance on Board of Directors' Effectiveness for Domestic Bank and Savings and Loan Holding Companies With Total Consolidated Assets of $50 Billion or More (Excluding Intermediate Holding Companies of Foreign Banking Organizations Established Pursuant to the Federal Reserve's Regulation YY), and Systemically Important Nonbank Financial Companies Designated by the Financial Stability Oversight Council for Supervision by the Federal Reserve.

[23] See 82 FR 39049 (August 17, 2017) for the proposed large financial institutions rating system (LFI rating system). For firms that would be subject to this guidance but not subject to the proposed LFI rating system, this guidance would help inform the Federal Reserve's evaluation of the firm's overall safety and soundness and the effectiveness of its risk management practices.

systemically important nonbank financial companies designated by the Financial Stability Oversight Council (FSOC) for supervision by the Board.

Application to Foreign Banking Organizations

Regulation YY requires FBOs with combined U.S. assets of $50 billion or more to maintain a U.S. risk committee to oversee the risk management framework of the combined U.S. operations.[24] Regulation YY also requires FBOs with U.S. non-branch assets of $50 billion or more to establish an intermediate holding company (IHC), which is governed by a board of directors or managers with equivalent rights, powers, privileges, duties, and responsibilities to those of a board of directors of a domestic corporation.[25] The Federal Reserve's expectations for governance of the combined U.S. operations of an FBO are generally consistent with its expectations for governance of large domestic firms and, in this guidance, a reference to "firm" should be taken also as a reference to the combined U.S. operations of an FBO, unless the context requires otherwise. Given that an FBO's combined U.S. operations are part of a larger global organization, the Federal Reserve anticipates that certain elements of an FBO's governance framework may be located outside of the United States. In this event, these elements should enable effective governance and risk management by the U.S. senior management, the U.S. risk committee, and the IHC board (as applicable), and should facilitate U.S. supervisors' ability to assess the adequacy of governance and controls in the combined U.S. operations.

Core Principles of Effective Senior Management, Management of Business Lines, and Independent Risk Management (IRM) and Controls

This guidance sets forth core principles of effective senior management, the management of a firm's business lines[26] and IRM and controls.[27]

I. Core Principles of Effective Senior Management

---

[24] 12 CFR 252.155(a).

[25] 12 CFR 252.153(a)(2)(ii).

[26] For a LISCC firm, due to its size, risk profile, and systemic importance, the guidance would apply to all of the firm's business lines. For an LFI that is not a LISCC firm, the expectations for management of business lines would apply only to business lines where a significant control disruption, failure, or loss event would result in a material loss of revenue, profit, or franchise value, or result in significant consumer harm. Other business lines of these firms which do not meet that definition would be expected to maintain appropriate risk management practices to ensure the firm's safety and soundness. The expectations included in this guidance relating to effective senior management oversight and IRM and controls would apply across the entire firm, and are not limited to the individual business lines that are subject to the expectations concerning the management of business lines.

[27] IRM and controls refers to a firm's independent risk management function, system of internal control, and internal audit function.

Principle: Senior management is responsible for managing the day-to-day operations of the firm and ensuring safety and soundness and compliance with internal policies and procedures, laws, and regulations, including those related to consumer protection.

Under the board's oversight, a firm's senior management is responsible for managing the day-to-day operations of the firm, and for ensuring safety and soundness and compliance with internal policies and procedures, laws, and regulations, including those related to consumer protection.[28] Two key responsibilities of senior management are overseeing the activities of the firm's business lines (individually and collectively) and the firm's IRM and controls.

Senior management is responsible for implementing the firm's strategy and risk tolerance approved by the board.[29] Senior management should implement the strategic and risk objectives across the firm to support the firm's long-term resiliency and safety and soundness, including the firm's ability to withstand the impact of a range of stressed conditions.[30] Senior management should ensure 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. Senior management should also 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.

---

[28] The term "senior management" refers to the core group of individuals directly accountable to the board of directors for the sound and prudent day-to-day management of the firm. 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.

"Board" or "board of directors" also refers to committees of the board of directors, as appropriate.

[29] See 82 FR 37219 (August 9, 2017). "Risk tolerance" is defined as 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.

For an FBO, the U.S. risk committee should approve the risk tolerance for the combined U.S. operations (which may be developed separately for the IHC and branch operations, respectively). The strategy for the combined U.S. operations may mean the manner in which the U.S. operations support the global strategy.

[30] 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. For example, a residential mortgage business unit should specify the level and type of credit risk, interest-rate risk, or other risks it plans to assume in its activities relative to the level and type specified in the risk tolerance.

Senior management is responsible for maintaining and implementing an effective risk management framework and ensuring the firm appropriately manages risk consistent with its strategy and risk tolerance.[31] This includes establishing clear responsibilities and accountability for the identification, measurement, management, and control of risk. Senior management is responsible for promoting and enforcing prudent risk-taking behaviors and business practices, including through the firm's compensation and performance management programs. 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.[32] Senior management should also periodically assess the risk management framework as a whole to ensure that the framework 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.

Senior management should ensure effective communication and information sharing across the entire firm. Senior management should also address any impediments to the effective flow of information, including those that could result in decisions being made or actions being taken in isolation.

In overseeing the firm's day-to-day operations, senior management should base its decisions and actions, as well as its communications with the board, on a full understanding of the firm's risks and activities. Therefore, senior management should have in place robust mechanisms for:

- Keeping apprised of drivers and trends related to current and emerging risks, material limit breaches, and other material issues;
- Maintaining and assessing the firm's system of internal control;
- Staying informed about material deficiencies and limitations in risk management and control practices, and ensuring that such deficiencies are remediated in a timely fashion;
- Assessing the potential impact of the firm's activities and risk positions on the firm's capital,[33] liquidity, and overall risk profile;

---

[31] For FBOs, regardless of whether a firm's senior management resides in the United States, senior management should fully understand the risks of U.S operations and communicate information on the risks of combined U.S. operations to global management so that these risks are included in the aggregate risk assessment of the global organization. Further, senior management with authority over budgeting or strategy for the combined U.S. operations should allocate appropriate resources and expertise to meet the expectations of this guidance.

[32] The term "internal controls" 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.

[33] References to "capital" in this section are not applicable to branches or agencies of an FBO.

- Assessing the firm's financial and nonfinancial performance relative to the firm's strategy and risk objectives;
- Maintaining robust management information systems to support oversight of the firm's activities and risk positions, and to provide information to the board; and
- Maintaining current succession and contingency staffing plans for key positions.

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. Further, senior management is responsible for ensuring resolution of risk management issues (including those identified by the firm and outstanding supervisory matters), escalating issues to the board, and communicating issues internally when appropriate. 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.

II. Core Principles of the Management of Business Lines

This section sets forth core principles of the management of business lines, including critical operations.[34] As used in this guidance, 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.[35]

For a LISCC firm, due to its size, risk profile, and systemic importance, these principles apply to all of the firm's business lines. For an LFI that is not a LISCC firm, these principles 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.

---

[34] A business line is 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. Under certain organizational structures, a business line may cross legal entities or geographic jurisdictions.

"Critical operations" are those operations, including associated services, functions and support, the failure or discontinuance of which, in the view of the firm or the Federal Reserve, would pose a threat to the financial stability of the United States. All of the expectations for the management of business lines apply to critical operations.

[35] 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.

A business line may cross legal entities or geographic jurisdictions. In instances where a business line of an FBO is part of a larger business conducted outside of the United States, expectations apply only to the portion of that business conducted in the United States.[36]

This section is organized as follows:

A. Implementation and Execution of Strategy and Risk Tolerance
B. Risk Identification and Risk Management
C. Resources and Infrastructure
D. Business Controls
E. Accountability

A. Implementation and Execution of Strategy and Risk Tolerance

Principle: Business line management should execute business line activities consistent with the firm's strategy and risk tolerance.

Business line management should establish specific business and risk objectives for each business line that align with the firmwide strategy and risk tolerance. Business line management should inform senior management when the business line's risk management capabilities are insufficient to achieve those business and risk objectives. In addition, during the strategic planning process with senior management, business line management should 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.

Business line management should 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.

B. Risk Identification and Risk Management

[36] Business line management of the U.S. operations should ensure that business line risks are captured comprehensively with consideration given to risks outside the United States that may impact the FBO's combined U.S. operations. Moreover, business line management should provide sufficient information to global management and escalate issues, as appropriate, to enable an understanding of the risks from the combined U.S. operations.

Principle: Business line management should identify, measure, and manage the risks associated with the business activities under a broad range of conditions, incorporating input from IRM.[37]

Business line management should identify, measure, and manage current and emerging risks that stem from the business line's activities and changes to external conditions.[38] Where it is difficult to assess risks quantitatively, business line management should still assess the impact of those risks, such as through qualitative means. These risks should include significant exposures and activities, both on-balance and off-balance sheet, and any other potential sources of risk related to the business line's activities. Business line management should incorporate appropriate feedback from IRM on business line risk positions, implementation of the risk tolerance, and risk management practices, including risk mitigation.

In measuring risks, business line management should consider the size and risk characteristics of the business line's exposures and business activities. Business line management should aggregate risks, including by business activities or products. For instance, management of a large commercial lending business line should understand risks affecting the business line as a whole, and also within segments of the business line, such as large corporate exposures, commercial real estate loans, and small business lending.

The activities of a business line should remain within risk limits established by IRM.[39] Business line management should consult with senior management before allowing any exceptions to risk limits.[40] This consultation should culminate in a well-supported decision by management to accept the risk or reduce its risk exposure. Business line management should subject any exceptions to risk limits to the firm's formal approval process. A business line may need to employ risk mitigation strategies to remain aligned with the firmwide strategy and risk tolerance.

A firm should have policies and procedures for vetting new business products and initiatives. Risks from new businesses should be identified and captured in risk management governance, infrastructure, compliance, and processes before commencing the new business. Business line management should escalate to senior management any required changes or modifications to risk management systems or internal control policies and procedures arising from the adoption of a new

---

[37] As noted in the Independent Risk Management and Controls section below, IRM is responsible for conducting a separate, objective, critical assessment of risks and risk-taking across the entire firm, separate from the business line's risk management activities.

[38] Emerging risks include those that have yet to create a material impact or would only arise during stressful or unlikely circumstances. The risk assessment should include all relevant risks, both financial and non-financial, including compliance risk.

[39] Business line management may develop its own limits for internal business line use and may provide input to 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 because the limits set by IRM should be the operative, formal, and binding across the firm.

[40] Business line management should evaluate breaches of risk limits to determine whether a breach represents a weakness in the monitoring or limits framework for the business lines, and take appropriate remedial action.

business or initiative. Additionally, growth in the new business should be consistent with the firm's risk management capabilities.

C. Resources and Infrastructure

Principle: Business line management should 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.

Business line management should 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, including stressful ones.[41] Sufficient resources and infrastructure include personnel with appropriate training and expertise and management information systems. Business line management should inform senior management if the business line's resources and infrastructure are insufficient to meet its business objectives.

Business line management should ensure that the business line's infrastructure is sound and appropriate for the intended specific business activities and that management information systems are sufficiently flexible to produce ad hoc and more frequent reporting when necessary. Business line management should address any gaps or weaknesses identified in the existing infrastructure and escalate to senior management if appropriate.

Business line management should ensure that the business line has:

- 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; and
- Succession and contingency plans for key positions.

Business line management should provide training and development to its staff to ensure sufficient knowledge of business line activities; compliance, operations and risk management processes; controls; and business continuity. Business line management should reinforce

---

[41] "Financial strength and resilience" is defined as 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" is defined as 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.

balanced risk-taking and provide incentives for appropriate behaviors through talent management processes, compensation arrangements, and other performance management processes.

D. Business Controls

Principle: Business line management should ensure that the internal control system is effective for the business line operations.

Business line management should develop and maintain an effective system of internal control for its business line that helps to ensure compliance with laws and regulations, including those related to consumer protection, and supports effective risk management.[42] For example, a business line's system of internal control should include access controls, change controls, and data integrity controls, including data reconciliations, variance analysis, and data quality logic checks. The system of internal control for a business line should be commensurate with the business line's size, scope of operations, activities, and risk profile. A comprehensive system of internal control includes policies, procedures, systems, and processes specific to the business line.

Business line management should regularly test to ensure the controls within its 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. Business line management should ensure that deficiencies in control design and operating effectiveness are remediated. Business line management should 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. Finally, business line management should reassess all key controls periodically to ensure relevancy and alignment with current approved policies.

E. Accountability

Principle: Business line management and staff are 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.

Business line management should establish policies and guidelines that specify accountability, set forth clear lines of management authority within the business line, and clearly align desired behavior with the firm's performance management incentives. Business line management should hold their staff accountable to the extent behavior that is inconsistent with the board and senior management directives and inform senior management as appropriate. Business line management should 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.

Business line management should have ongoing and effective means to prevent, detect, and remediate risk management and compliance failures of business line policies and procedures, as

[42] In developing and maintaining its system of internal control, a business line may use the internal controls that are in place across the firm.

well as policies and limits established by the firm's senior management. Business line management should develop processes with indicators and early warning mechanisms to facilitate timely detection of existent and potential issues. Business line management should actively supervise employees in light of the firm's policies and guidelines.

III. Core Principles of Independent Risk Management and Controls

There are three key areas covered in this section: (1) IRM, which provides an objective, critical assessment of risks and evaluates whether a firm remains aligned with its stated risk tolerance; (2) a system of internal control to guide practices, provide appropriate checks and balances, and confirm quality of operations; and (3) internal audit, which provides independent assessments of the effectiveness of the risk management framework and the system of internal control.

This section is organized as follows:

A. Governance, Independence, and Stature
    1. Chief Risk Officer (CRO)
    2. Chief Audit Executive (CAE)
B. Independent Risk Management
    1. Risk Tolerance and Limits
    2. Risk Identification, Measurement, and Assessment
    3. Risk Reporting
C. Internal Controls
D. Internal Audit

Except for the roles of the CRO and the CAE, this guidance does not purport to prescribe in detail the governance structure for a firm's IRM and controls. Senior management should establish and maintain clear lines of responsibility and accountability so that activities are conducted in a manner that satisfies supervisory expectations.

Supervisory expectations related to independent risk management apply to the U.S. CRO and the U.S. risk committee of an FBO for the combined U.S. operations in the same manner as these expectations apply to the CRO and risk committee of a domestic holding company. For an FBO, the internal audit function for the combined U.S. operations should have appropriate independent oversight of those.

A. Governance, Independence, and Stature[43]

[43] "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.

1. Chief Risk Officer

Principle: The CRO should establish and maintain IRM that is appropriate for the size, complexity, and risk profile of the firm.

The Board's Regulation YY requires certain firms to have a CRO with sufficient capability and experience in identifying, assessing, and managing risk exposures of large, complex financial institutions.[44] To promote the stature and independence of IRM, the CRO must report directly to the board's risk committee as well as to the CEO.[45] The CRO also must provide reports to the board's risk committee at least quarterly.[46]

As part of overseeing IRM, the CRO should guide IRM to establish and monitor compliance with enterprise-wide risk limits, identify and aggregate the firm's risks, assess the firm's risk positions relative to the parameters of the firm's risk tolerance, and provide relevant risk information to senior management and the board. The CRO should also oversee communication of the firm's risk limits to the board and relevant firm management and staff.

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.[47] Further, the CRO should be included in discussions with other senior management and the board related to key decisions such as strategic planning and capital and liquidity planning. The CRO should also provide input to the board on incentive compensation plan design and effectiveness.

The CRO should escalate issues to senior management and the board when activities or practices at the firmwide, risk-specific, and business-line level do not align with the firm's overall risk tolerance. For example, the CRO should report concerns to the board's risk committee if the firm does not have sufficient risk management capacity to enter into a proposed merger or new product line and promote the taking of appropriate actions, as warranted. The CRO should recommend constraints on risk-taking and enhancements to risk management practices to senior management and the board. The CRO or IRM should be involved in any proposal to waive or make exceptions to established risk limits, including on a temporary basis, should provide an assessment of any such proposal, and should escalate the proposal to the board of directors as

---

[44] 12 CFR 252.33(b); 12 CFR 252.155(b). For an FBO, references to CRO and risk committee mean the U.S. CRO and U.S. risk committee required under 12 CFR 252.155.

[45] 12 CFR 252.33(b)(3)(ii). For an FBO, the U.S. CRO must report to the U.S. risk committee and the global CRO or equivalent management official(s) who is responsible for overseeing the implementation of and compliance with policies and procedures relating to risk management governance, practices, and risk controls of the FBO (unless the Federal Reserve approves an alternate reporting structure). 12 CFR 252.155(b)(3).

[46] 12 CFR 252.33(a)(3)(v). This requirement does not apply to the U.S. CRO of an FBO.

[47] Other officers of the firm may oversee portions of functions involved in risk management and control activities.

appropriate. The necessary level of approval within IRM and escalation should be clearly articulated in policies and procedures and commensurate with the nature of the risk limit.

The CRO should support the independence of IRM from the business lines by establishing clearly defined roles and responsibilities, and reporting lines. The CRO should periodically assess whether IRM has appropriate staffing and systems; sufficient understanding of the risks and business activities being evaluated; and sufficient authority to identify and escalate material or persistent risk management and control deficiencies and to challenge senior management and business line management when warranted.

2. Chief Audit Executive

Principle: 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.

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.[48] The CAE should effectively manage all aspects of internal audit work on an ongoing basis, including any internal audit work that is outsourced. The CAE should have the authority to oversee all internal audit activities and to hire internal audit staff with sufficient capability and stature. Under the direction of the CAE, the internal audit function performs independent assessments of the effectiveness of the firm's system of internal control and the risk management framework. The CAE should report findings, issues, and concerns to the board's audit committee and senior management.

[48] See SR letter 13-1/CA letter 13-1, "Supplemental Policy Statement on the Internal Audit Function and Its Outsourcing."

B. Independent Risk Management[49]

1. Risk Tolerance and Limits

Principle: 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.

IRM should provide input into and evaluate the firm's risk tolerance to ensure that it appropriately captures the firm's material risks and aligns with the firm's strategy and the corresponding business activities.[50] In addition, IRM should evaluate whether the risk tolerance:

- Addresses risks under normal and stressed conditions and considers changes in the risk environment;
- Includes risks associated with the firm's revenue generating activities, as well as other aspects of risks inherent to the business, such as compliance, information technology, and cybersecurity;
- Incorporates realistic risk and reward assumptions that, for example, do not overestimate expected returns from business activities or underestimate risks associated with business activities; and
- Guides the firm's risk-taking and risk mitigation activities.

IRM should determine whether the firm's risk profile is consistent with the firm's risk tolerance and assess whether the firm's risk management framework has the capacity to manage the risks outlined in the risk tolerance. Specifically, IRM should 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.

Principle: IRM should establish enterprise-wide risk limits consistent with the firm's risk tolerance and monitor adherence to such limits.

Under direction of the CRO, IRM should establish enterprise-wide risk limits that are consistent with the firm's risk tolerance for the firm's full set of risks, including risks associated with

---

[49] Independent risk management is comprised of a range of risk management functions. For example, firms should have an independent compliance risk management function that establishes a firmwide compliance risk management program and delineates responsibilities for managing compliance risk. See SR letter 08-08/CA letter 08-11, "Compliance Risk Management Programs and Oversight at Large Banking Organizations with Complex Compliance." The structure and reporting lines for such an independent compliance risk management function may vary across firms.

[50] The development and ongoing update of a firm's risk tolerance is an iterative process, meaning that several parties provide input on a continual basis. IRM's input into and evaluation of the risk tolerance should fit into this overall process and may occur at several different stages.

revenue generating activities and those inherent to the business. 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. For example, risk limits can cover single counterparty credit exposures, funding concentrations, country exposures, or subprime lending activities. Risk limits should be clear, relevant, and current. IRM should create lower-level risk limits, such as for an individual business line, based on the enterprise-wide risk limits.

Risk limits should be quantitative and qualitative. For instance, quantitative limits can be set relative to earnings, assets, liabilities, capital, liquidity, or other relevant benchmarks. IRM should set qualitative limits – such as an expert assessment to constrain business in a given country – as a proxy for risks or aspects of risks that are more difficult to quantify. Risk limits should include explicit thresholds that, if crossed, strictly prohibit the activity generating the risk.

To the extent possible, risk limits should:

- 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; and
- Reinforce compliance with laws and regulations, including those related to consumer protection, and consistency with supervisory expectations.

IRM should monitor and update risk limits as appropriate, especially as the firm's risk tolerance is updated, the firm's risk profile changes, or external conditions change. IRM should also identify significant trends in risk levels to evaluate whether risk-taking and risk management practices are consistent with the firm's strategic objectives. IRM should escalate to senior management any material breaches of the firm's enterprise-wide risk limits and risk tolerance, as well as instances where IRM's conclusions differ from the conclusions of a business line.

2. Risk Identification, Measurement, and Assessment

Principle: IRM should identify and measure the firm's risks.

IRM's activities are conducted in addition to business line risk management activities described above and should provide an objective, critical perspective of a firm's risks. IRM should identify and measure current and emerging risks within and across business lines and risk types, as well as any other relevant perspectives, such as by legal entity or jurisdiction. Where it is difficult to assess risks quantitatively, IRM should still assess the impact of those risks, such as through qualitative means. IRM should conduct its risk identification and measurement work on an ongoing basis to reflect any changes in exposures, business activities, and the broader operating environment, including changes in law and supervisory expectations.

IRM should identify risk types, including credit, market, operational, liquidity, interest rate, legal, compliance and related risks (such as consumer protection and Bank Secrecy Act/anti-

money laundering). IRM should establish minimum internal standards for all of its risk identification and measurement practices to ensure consistent quality across different risks. IRM's standards should include both quantitative and qualitative elements, with the latter especially important for risks or aspects of risks that are more difficult to quantify. The standards at a firm should be dynamic, inclusive, and comprehensive.

To conduct effective risk identification and measurement, IRM should have access to timely, reliable, and comprehensive information about all risk-related exposures and activities in the firm. This should include emerging or potential sources of risk. IRM should seek input across the firm in identifying risks. IRM may utilize information collected or used from business lines; however, IRM 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.

IRM should regularly measure identified risks under both normal and stressful operating conditions. In measuring risks, IRM should consider the size and risk characteristics of the firm's exposures and business activities. Within each risk type, IRM should rely on a range of metrics and use measures appropriate to different risk types.

Principle: IRM should aggregate risks and provide an independent assessment of the firm's risk profile.

IRM should aggregate risks across the entire firm and assess those risks relative to the firm's risk tolerance.[51] IRM should identify material or critical concentrations of risks and assess the likelihood and potential impact of those risks on the firm. Further, IRM should identify activities or exposures that have related risk factors and assess the combined impact of those risk factors on the firm. IRM should assess risk information along different meaningful dimensions at a more granular level than firmwide, such as by business line, geographic regions, obligors, counterparties, and products, to determine how those impact the firm's risk profile.

IRM should 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. IRM should assess risks and risk drivers within and across business lines and risk types, as well as any other material perspectives, such as by legal entity or jurisdiction. Further, IRM should analyze any assumptions related to risk diversification. IRM also should assess risk mitigation strategies, including the effectiveness of such mitigation in a range of circumstances, and recommend alternatives if concerns arise.

IRM should identify information gaps, uncertainties, and limitations in risk assessments for senior management, and as appropriate, for the board. For instance, in analyzing a new product area or business line, IRM should acknowledge areas of insufficient information that limit a complete assessment of the risks and provide a measured implementation plan to obtain the necessary information.

---

[51] For example, IRM should be able to aggregate all retail credit risk across the firm's different consumer business lines (such as credit cards, residential mortgages, and auto lending).

3. Risk Reporting

Principle: IRM should 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 be comprehensive, useful, accurate, and timely. Risk reporting should cover current and emerging risk and adherence to risk limits and risk concentrations as well as 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; and support or influence strategic decision-making. Risk reporting should provide information on aggregate risks within and across business lines and risk types, as well as by legal entity or jurisdiction and significant concentrations.

Risk reporting should be tailored to meet the differing information needs of the board, senior management, and others within the firm. The frequency of reporting should depend on needs of the firm and the materiality of the issues. Risk reporting should adapt to market downturns or stress events.

C. Internal Controls

Principle: 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 consistent with all applicable laws and regulations, including those related to consumer protection.

Internal controls cover a wide range of activities and processes, and could include the following:[52]

- Policies and procedures that set expectations for and govern the firm's business activities and support functions; establish appropriate levels of authority, responsibility, and accountability for overseeing and executing the firm's activities; and establish standards for prudent risk-taking behaviors.
- Clear assignment of roles and responsibilities and appropriate separation of duties.
- Physical controls for restricting access to tangible assets.
- Approvals and appropriate dual authorizations for key decisions, transactions, and execution of processes.
- Verifications of transaction details and periodic reconciliations, such as those comparing cash flows to account records and statements.
- Access controls, change management controls, data entry and related controls.

[52] See SR letter 03-5, "Amended Interagency Guidance on the Internal Audit Function and its Outsourcing."

- Escalation procedures with a system of checks and balances in situations that allow for managerial or employee discretion.

Internal controls instill confidence in financial reporting and are important to ensure the integrity of the process and information relied upon by the firm to manage itself. Developing and maintaining an effective system of internal control is the responsibility of several parties, including business line management.[53] Accordingly, a firm should assign management responsibilities for the establishment and maintenance of 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. All personnel should fully understand and adhere to policies and procedures affecting their duties and responsibilities.

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

A firm should have mechanisms to test its system of internal control and to identify and escalate issues that appear to compromise its effectiveness. A firm should regularly evaluate and test the quality, reliability and effectiveness of internal controls, and monitor any potential deterioration. Generally, testing activities are conducted at specific points in time, whereas monitoring activities are continuous processes. The scope, frequency, and depth of testing should consider the complexity of the firm, the results of the firm's 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.

A firm should evaluate and communicate internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management. Firms should establish management information systems that track internal control weaknesses and escalate serious matters to the board, senior management, and responsible business line management, as appropriate.

D. Internal Audit

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.

An effective internal audit function provides independent assurance to the board and senior management concerning the effectiveness of risk management and internal control systems. The Federal Reserve issued guidance outlining the key components of an effective internal audit function in SR letter 03-5, and followed that with supplemental guidance in SR letter 13-1/CA letter 13-1, "Supplemental Policy Statement on the Internal Audit Function and Its Outsourcing." The supplemental guidance builds upon the 2003 interagency guidance of SR letter 03-5 and

[53] As described below, the internal audit function should examine, evaluate, and perform an independent assessment of the firm's internal control system.

further addresses the characteristics, governance, and operational effectiveness of a firm's internal audit function. That existing audit guidance remains in place and is not superseded by this guidance.

By order of the Board of Governors of the Federal Reserve System, January 3, 2018.

Ann E. Misback,
Secretary of the Board.