The Institute of Internal Auditors

Richard F. Chambers
Certified Internal Auditor
Qualification in Internal Audit Leadership
Certified Government Auditing Professional
Certification in Control Self-Assessment
Certification in Risk Management Assurance
President and Chief Executive Officer

T: +1-407-937-1200
E-mail: richard.f.chambers@theiia.org

February 26, 2018

Ann E. Misback
Secretary, Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue NW
Washington, DC 20551

Response e-mailed to: regs.comments@federalreserve.gov

RE: Docket No. OP-1594

Dear Ms. Misback:

Thank you for the opportunity to comment on Proposed Supervisory Guidance to clarify the Federal Reserve expectations related to risk management for large financial institutions. The Institute of Internal Auditors (IIA) represents more than 190,000 internal auditors engaged around the globe in good governance for organizations of all sizes. On behalf of our members and our Board of Directors, The IIA supports the Proposed Supervisory Guidance regarding the management of business lines and independent risk management for large financial institutions.

In October 2017, The IIA provided its support of Part One of the guidance related to oversight of a firm by its board of directors, as it closely mirrors The IIA's efforts to elevate the profession through the *International Professional Practice Framework* (IPPF).

Similarly, the IPPF and its *International Standards for the Professional Practice of Internal Auditing* inform our support here, specifically in response to three of the questions in the Requests for Comments section on pages 14-15, as follows:

Question 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 Independent Risk Management (IRM) be clarified?***

Federal Reserve guidance set forth in section I, Core Principles of Effective Senior Management (page 20), explains that "*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.*" We agree that it is senior management's responsibility to report risk and control issues to the board. We also

Global Headquarters
1035 Greenwood Blvd, Suite 401
Lake Mary, FL 32746 USA
T: +1-407-937-1100
F: +1-407-937-1101
www.theiia.org

agree that senior management is ultimately responsible for the firm's risk management framework. However, per IIA Standard 1111: Direct Interaction with the Board, we believe it would be beneficial to acknowledge in this section that the Chief Audit Executive (CAE), as the independent representative of the third line of defense, is expected to report risk and control issues to the board, as well. Standard 1111 states, "The chief audit executive must communicate and interact directly with the board." This view is already reflected in the Federal Reserve guidance section III, Core Principles of Independent Risk Management and Controls, 2. Chief Audit Executive (page 30), specifically: "*The CAE should report findings, issues, and concerns to the board's audit committee and senior management*." We believe that including it earlier in section I of Core Principles of Effective Senior Management will serve to clarify the guidance.

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

Federal Reserve guidance set forth in section III, Core Principles of Independent Risk Management and Controls, 2. Chief Audit Executive (page 30), explains the principle that "*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*." We agree with this principle, as we take this to mean that internal audit should be empowered to hire adequate personnel with required skill sets as appropriate to the size, complexity, and risk profile of the firm. This guidance follows IIA Standard 1210: Proficiency, which states, "Internal auditors must possess the knowledge, skills, and other competencies needed to perform their individual responsibilities. The internal audit activity collectively must possess or obtain the knowledge, skills, and other competencies needed to perform its responsibilities."

Furthermore, the Federal Reserve guidance set forth in D. Internal Audit (page 35) explains the principle that "*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."* We believe this principle to be accurate, as reflected in IIA Standard 2120: Risk Management, and IIA Standard 2130: Control. Standard 2120 states, "The internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes;" and Standard 2130: Control states, "The internal audit activity must assist the organization in maintaining effective controls by evaluating their effectiveness and efficiency and by promoting continuous improvement." Additionally, we note that SR 13-1 Supplemental Policy Statement on the Internal Audit Function and Its Outsourcing already provides extensive guidance relevant to this section.

Question 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?***

The IIA believes that, while the terms *risk appetite* and *risk tolerance* are currently used interchangeably within the industry, they are not necessarily synonymous. According to the IPPF, The IIA defines *risk appetite* as, "The level of risk that an organization is willing to accept." While The IIA does not define *risk tolerance*, The Committee of Sponsoring Organizations of the Treadway Commission (COSO), of which The IIA is a part, defines *risk tolerance* as, "The acceptable variation in outcomes related to specific performance measures that are linked to objectives the entity seeks to achieve.[1]" While some supervisors have chosen not to use *risk tolerance* in their vocabulary, The IIA still sees value in differentiating the two terms, especially in the financial services context. When used in operations environments, we tend to see the term *risk tolerance* used to indicate acceptable risk exposure variations around a given objective, while *risk appetite* tends to be used in the context of fixed limits for risk exposure or for the statement explaining the static risk exposures

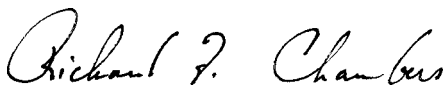
[1] Beasley, Mark S., Bonnie V. Hancock, and Bruce C. Branson for Committee of Sponsoring Organizations of the Treadway Commission. *Strengthening Enterprise Risk Management for Strategic Advantage* (Durham, North Carolina: American Institute of CPAs), 2009.

that financial services firms will accept for categories of assets and liabilities. For example, when discussing risk exposures at a detailed level, such as individual trades, depending on the underlying asset, there will be intraday volatility that may be difficult to manage at that level. Defining and using *risk tolerance* in this way allows the firm to be much more specific when designing risk limits and other escalation protocols while still considering the limitations traders have in managing the value of their trades on a daily basis. In this scenario, *risk appetite* continues to be the driving framework used by the board and senior management to manage overall risk exposure in the organization.

We note that you have used the term *"risk objectives"* in the document to designate "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." This comes close to the definition of *risk tolerance* we are advocating; however, *risk objectives* could still be used as an intermediate term to apply to business lines and broad categories of risk, such as "credit risk objectives for auto loans." We recommend using *risk tolerance* to refer to volatility.

We appreciate the Federal Reserve's consideration of our comments. If you have any questions about our response or would like to discuss further, please contact Kathy Anderson, The IIA's Managing Director of North American Advocacy. Ms. Anderson can be reached at kathy.anderson@theiia.org or 407-937-1291.

Sincerely,



Richard F. Chambers, CIA, QIAL, CGAP, CCSA, CRMA
President & Chief Executive Officer

About The Institute of Internal Auditors
The Institute of Internal Auditors (IIA) is the internal audit profession's most widely recognized advocate, educator, and provider of standards, guidance, and certifications. Established in 1941, The IIA today serves more than 190,000 members from more than 170 countries and territories. The association's global headquarters are in Lake Mary, Fla. For more information, visit www.theiia.org.