THE RISK MANAGEMENT ASSOCIATION

1801 Market Street, Suite 300 • Philadelphia, PA 19103
215-446-4000 • Fax: 215-446-4101 •
www.rmahq.org

VIA E-MAIL: regs.comments@federalreserve.gov

March 14, 2018

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

Re: Docket ID OP-1594, "Proposed Guidance on Core Principles of (i) Effective Senior Management; (ii) Management of Business Lines; and (iii) Independent Risk Management and Controls" (the "Proposed Guidance")

Ladies and Gentlemen:

This letter is submitted by The Risk Management Association ("RMA" or the "Association") in respect of the Proposed Guidance issued by the Board of Governors on January 3, 2018, which would establish principles regarding effective senior management; management of business lines; and independent risk management and controls.

Introduction

RMA is a 501(c)(6) not-for-profit, member-driven professional association whose sole purpose is to advance the use of sound risk management principles in the financial services industry. RMA helps its members use sound risk management principles to improve institutional performance and financial stability and enhance the risk competency of individuals through information, education, peer-sharing and networking. RMA has 2,500 institutional members that include banks of all sizes as well as nonbank financial institutions. They are represented in the Association by more than 18,000 risk management professionals who are chapter members in financial centers throughout North America, Europe, Asia, and Australia.

This letter is divided into two parts:

- Part I contains RMA's responses to the question posed by the Federal Reserve in the Proposed Guidance regarding the definition of the term "risk tolerance."

- Part II sets forth other commentary directed at certain provisions of the Proposed Guidance.

1801 Market Street, Suite 300 • Philadelphia, PA 19103
215-446-4000 • Fax: 215-446-4101 •
www.rmahq.org

One of the most important components of RMA's mission is to provide independent analysis on matters pertaining to risk and capital regulation. In this regard, the comments contained herein are informed by subject matter experts from member institutions of the Association, but are not attributable to any single institution or group of institutions, some of whom may file their own comment letters.

PART I -- Responses to Certain Questions Presented

Question: 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?

ANSWER: The Proposed Guidance provides that "(s)enior management is responsible for implementing the firm's strategy and *risk tolerance* (emphasis added) approved by the board." Moreover, the Proposed Guidance defines the term "risk tolerance" 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."[1]

RMA respectfully suggests that the Federal Reserve is conflating the meaning of the term "risk tolerance" with the concept of "risk appetite." Simply put, risk appetite should be defined as the amount of risk, or volatility of results, a firm is willing to accept in pursuit of a desired return.[2] Risk tolerance, on the other hand, is the broadest expression of risk that an institution is willing to assume in the execution of its strategy. RMA believes that it is critical for the Federal Reserve to be clear when it defines terms.

The concepts of risk appetite and risk tolerance are often used interchangeably, but they have distinct differences in meaning. Risk appetite represents the acceptance of volatility that an institution is willing to assume in executing its business strategy. Risk tolerance refers to the day-to-day operational limits developed within the context of an institution's stated risk appetite (for example, concentration limits) and can be understood visually by reference to the diagram set forth below.

[1] Proposed Guidance at footnote 29.
[2] Risk Appetite Workbook, A Framework for Setting Risk Appetite, published by The Risk Management Association (2010). At page 3. RMA's Risk Appetite Workbook was developed by a working group comprised of senior risk professionals from international, large, regional, and mid-tier institutions, as well as community banks.

1801 Market Street, Suite 300 • Philadelphia, PA 19103
215-446-4000 • Fax: 215-446-4101 • www.rmahq.org

The treatment above is consistent with the approach taken by COSO[3], which defines the terms "risk appetite" and "risk tolerance" as follows:

- Risk Appetite is "the amount of risk, on a broad level, that an organization is willing to accept in pursuit of stakeholder value."
- Risk Tolerance "reflects the acceptable variation in outcomes related to specific performance measures linked to objectives the entity seeks to achieve."

The use of the term "risk appetite," instead of "risk tolerance," is also consistent with the OCC's Heightened Standards regulation, which provides that an institution should have a comprehensive written statement outlining its risk appetite that serves as the basis for the risk governance framework, containing qualitative components that define a safe and sound risk culture and how the covered bank will assess and accept risks and quantitative limits that include sound stress testing processes and address earnings, capital, and liquidity.[4] RMA respectfully submits that the Federal Reserve, wherever possible, harmonize taxonomies and standards with the OCC's heightened standards rule to avoid unnecessary confusion or duplication on the part of the institutions that they each supervise.

Simply put, there will be considerable confusion across the industry and with examiners if the Federal Reserve defines "risk tolerance" in essentially the same manner as the OCC defines the term "risk appetite." The Proposed Guidance also uses the term "risk objectives," which is an undefined term that has the potential to create additional confusion. For example, how does the term "risk objectives" relate to the term "risk limits."

[3] COSO – The Committee of Sponsoring Organizations, whose mission is to provide thought leadership through the development of frameworks and guidance on enterprise risk management, internal controls, and fraud deterrence.
[4] 54542 Federal Register / Vol. 79, No. 176 / Thursday, September 11, 2014 / Rules and Regulations.

THE RISK MANAGEMENT ASSOCIATION

1801 Market Street, Suite 300 • Philadelphia,
PA 19103
215-446-4000 • Fax: 215-446-4101 •
www.rmahq.org

PART II – Additional Commentary

RMA is supportive of the Federal Reserve's determination that the Proposed Guidance is necessary to refocus senior management, the management of business lines, and independent risk management on their respective core responsibilities. RMA appreciates this opportunity to comment on the Proposed Guidance and requests that the Federal Reserve take a principles-based, as opposed to a prescriptive, approach to the supervisory oversight of the effectiveness of senior management, management of business lines, and independent risk management. RMA believes that the Federal Reserve should focus attention on the "outcome" of practices by these distinct constituencies rather than attempting to prescribe the procedures to be followed by senior management, management of business lines, and independent risk management subject to the Proposed Guidance so that publication of the final version of the Proposed Guidance does not simply result in a compliance exercise. Finally, RMA respectfully suggests that it is important for the Federal Reserve to harmonize not only its expectations of senior management, management of the business lines, and independent risk management with the OCC's heightened standards, but also to harmonize its terminology with the OCC's. For example, the OCC's heightened standards rule uses the term "front line units" whereas the Proposed Guidance uses the term "business lines."

A. Core Principles of Effective Senior Management

We note that the term "senior management" is used throughout the Proposed Guidance and 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."[5] RMA agrees that the definition broadly captures the individuals that are primarily entrusted with executing an institution's strategic plan. RMA suggests that the Federal Reserve permit institutions to take a principles-based approach by permitting institutions to determine which individuals are specifically included in the group referred to as "senior management". We also note that institutions varyingly use the terms "senior management" and "executive management" interchangeably to refer to the individuals identified in the foregoing definition. Accordingly, we respectfully submit that in order to avoid confusion when the resulting guidance is applied by field examiners, that the term be codified in the final guidance as "senior or executive management" to avoid confusion with respect to individual institutions' naming conventions.

[5] Proposed Guidance, footnote 28.

THE RISK MANAGEMENT ASSOCIATION

1801 Market Street, Suite 300 • Philadelphia, PA 19103
215-446-4000 • Fax: 215-446-4101 •
www.rmahq.org

The core principles of effective senior management require that clear responsibilities and accountability be established for "the identification, measurement, management, and control of risk."[6] RMA respectfully submits that the concept of "control" of risk be broadened to include the concepts of risk acceptance, transfer, and mitigation as such concepts align with an institution's risk tolerance, which (as noted in Part I above) is developed and set within the context of an institution's stated risk appetite.

We also note that senior management is responsible for providing timely, ***useful*** (emphasis added), and accurate information to the Board. As you know, RMA previously submitted a comment letter dated October 6, 2017, regarding the Federal Reserve's Proposed Guidance on Enhancing the Effectiveness of Boards of Directors. RMA is concerned that boards are (i) facing increasing documentation burdens and (ii) increasing their scope or mandate beyond their advisory and oversight functions into actual management of the institution. RMA notes that the American Association of Board Directors has identified over 800 legislative and regulatory provisions that have accumulated over many decades that impact the responsibilities of bank directors. We submit that the ever-increasing regulatory burden creates a significant distraction from board time necessary for effective risk oversight and other essential board responsibilities. This also creates an increasing burden on senior management which must document static risks. In discharging their risk oversight function, boards should monitor bank performance against risk appetite and other metrics established pursuant to key policies approved by the board or its committees. Bank boards should be receiving high level information and key risks of concern in the context of informative and actionable reports from management. However, it is management which is responsible for managing risk, not the board which is charged with risk oversight.

We note that the Core Principles of the Management of Business Lines creates an expectation that the management of the business line provide training for personnel. RMA respectfully suggests that prudent risk management dictates that senior management should ensure that business line management has the resources necessary to train new and existing employees regarding the importance of professional conduct and compliance with laws and regulations, including those related to consumer protection.

B. Core Principles of the Management of Business Lines

RMA agrees that one of the core principles of effective business line management is that business line management should execute business line activities consistent with the firm's strategy and "<u>risk appetite</u>." The Proposed Guidance uses the term "risk tolerance" instead of the more

[6] Proposed Guidance, page 22.

1801 Market Street, Suite 300 • Philadelphia,
PA 19103
215-446-4000 • Fax: 215-446-4101 •
www.rmahq.org

accurate term "risk appetite" and we respectfully suggest that the Federal Reserve avoid conflating the meanings of the two terms as discussed in Part I above.

Institutions are subject to risk drivers, events and consequences or impacts, all of which may be mitigated by the application of controls. Controls may be characterized as preventative in instances where their application reduces the likelihood of an event; or detective, in cases where their application informs about the occurrence of an event; or corrective, in situations where their application reduces the impact or consequence of an event. It is important to note that the control environment should not remain static given the emergence of new and material risks. RMA believes that the line of business should own the risks associated with the business and correspondingly should be responsible for implementing controls commensurate with the institution's risk appetite. While business line management should ensure that its internal control system is effective, as stated in the Proposed Guidance, RMA respectfully suggests that the Proposed Guidance must also recognize that a business line may make the decision to relax or eliminate certain controls as it determines that it has excess capacity with respect to its risk appetite subject to the institution's standard protocols.

RMA notes that the final guidance could create confusion in terms of first line and second line responsibilities, require the unnecessary duplication of work across the first and second lines of defense, and cause the unnecessary expenditure of resources. In particular, as presently drafted, the Proposed Guidance would likely result in duplicative and overlapping structures and work being performed by both the first and second lines. By way of example, compare the business line's responsibilities to identify, measure and aggregate risks with IRM's responsibilities to identify, measure and aggregate risks.

C. Core Principles of Independent Risk Management and Controls

We note that the Proposed Guidance provides that the CRO should provide input to the Board on incentive compensation plan design and effectiveness. We ask that the Federal Reserve provide clarification regarding whether the input required of the CRO regarding incentive plan design and effectiveness is intended to be prospective; i.e., that the incentive compensation will be effective; and/or retrospective; i.e., whether the incentive compensation plan is functioning as intended.

The Proposed Guidance is very prescriptive regarding the concept of risk limits. A limit is simply a designated threshold or guidepost by which a firm would monitor its risk exposures to ensure that actual risk does not deviate materially therefrom. In the event that a risk limit is breached, an institution would generally initiate remedial action. The Proposed Guidance is extremely

1801 Market Street, Suite 300 • Philadelphia, PA 19103
215-446-4000 • Fax: 215-446-4101 • www.rmahq.org

prescriptive with respect to the application of risk limits, which provides that "risk limits should include explicit thresholds that, if crossed, strictly prohibit the activity generating the risk." RMA notes that most risk limits are designed to be crossed or exceeded and institutions have governance processes in place to grant exceptions to limits and/or undertake remedial action. Accordingly, the strict prohibition on exceeding a threshold should be deleted and should be replaced with a principles-based standard.

Should there be any questions concerning the comments reflected above, kindly contact Edward J. DeMarco, Jr., General Counsel and Director of Regulatory Relations at (215) 446-4052 or edemarco@rmahq.org.

Very truly yours,

Edward J. DeMarco, Jr.,
General Counsel & Director of Regulatory Relations