THE RISK MANAGEMENT ASSOCIATION
Serving the Financial Services Industry

1801 MARKET STREET, SUITE 300 • PHILADELPHIA, PA 19103 • 215-446-4000 • FAX 215-446-4101 • www.rmahq.org

William F. Githens, CRC
President & CEO

April 30, 2012

Via E-Mail: regs.comments@federalreserve.gov
Jennifer J. Johnson, Secretary
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue, NW
Washington, DC 20551

Re: Enhanced Prudential Standards and Early Remediation Requirements for Covered Companies, Regulation YY; Docket No. 1438, RIN 7100-AD-86

Response of The Risk Management Association

The Risk Management Association ("RMA") appreciates this opportunity to respond to Subpart E—Risk Management of the above-referenced proposed rules, which would implement the Risk Management and Risk Committee Requirements to be established under Section 165 of the Dodd-Frank Wall Street Reform and Consumer Protection Act ("Dodd-Frank Act" or the "Act").

RMA is a 501(c)(6) not-for-profit professional association whose sole purpose is to advance the use of sound risk principles in the financial services industry. RMA agrees that the use of sound, enterprise-wide risk management principles by Covered Companies (as defined below) should reduce the likelihood of their material distress or failure, thereby promoting financial stability. RMA also agrees with the Senior Supervisors Group that effective oversight of an organization as a whole is one of the most fundamental requirements of prudent risk management.

RMA supports the three lines of defense as a best practice for risk governance by Covered Companies, wherein: the first line of defense is promotion of a strong risk culture by senior management; the second line of defense is an independent, enterprise-wide risk management function; and the third line of defense is internal audit, which is charged with independent review and challenge of the first two lines of defense.

Introduction

RMA recognizes that a well-functioning financial system requires banks to take prudent risk positions that generate an appropriate level of earnings. An institution's risk level should be informed by its risk appetite. As the industry recovers from the economic crisis, institutions must focus on their risk tolerances so they become a part of the bank's risk culture.

RMA supports measures taken by financial institutions, particularly large, complex financial companies, that: (a) encourage an enterprise-wide view of risk management and a commensurate level of engagement throughout the organization, driven by an effective risk culture established by the board of directors and senior management; (b) establish well-defined roles and responsibilities for the identification, assessment, management, measurement, and reporting of risk, inclusive of robust governance; (c) adequately fund, staff, train, and empower risk management; (d) designate an executive level officer responsible for implementing and maintaining an enterprise-wide risk management framework; (e) ensure that a level of risk management competency exists throughout the organization, especially among senior managers, commensurate with the company's capital structure, risk profile, complexity, activities, size, and other appropriate risk-related factors; (f) ensure access to and use of high-quality, scalable data to inform decisions; and (g) establish a dedicated risk management committee of the board of directors. These points are compatible with the Board's general goals of facilitating risk management on an enterprise-wide basis and establishing clear accountabilities. Further, we feel these points are consistent with sound risk management practice, exclusive of any regulatory requirement or the then-current economic environment.

RMA believes that a sound risk management framework, one that addresses the risk management failures observed during the recent crisis, must exhibit a strong risk culture. The risk culture is a function of leadership and is most evident in setting the risk appetite of the institution. Informed decisions must be made in regard to the level and types of risk the institution is willing to tolerate, both on- and off-balance sheet. The board of directors and senior management must communicate the institution's risk expectations to stakeholders and regulators. An institution's risk culture is vital to ensure that decisions approved at the senior level are carried out appropriately. Senior line and risk officers must work together to convey the risk culture message throughout the institution. When properly coordinated, a robust risk management framework can serve as a guidepost in setting strategy; aligning people, processes, and infrastructure; helping to embed a risk culture; and guiding an institution in allocating resources to align its strategic plan, risk plan, and capital plan.

RMA believes the financial system is best served by thoughtful risk management processes and procedures that are principles-based and that consider multiple measures of risk and multiple means to control risk. In short, a thoughtful, principles-based approach encourages diversity of thought on risk management and allows financial institutions to implement risk management processes and procedures commensurate with their risk appetites, size, and complexity. In light of the foregoing, RMA believes several portions of the proposed rules are unnecessarily prescriptive and potentially disruptive, and would not provide the Board with the sought-after assurance of addressing the risk management failures observed during the recent crisis.

Risk Committee Requirements -- Documentation

Section 252.126(c) of the proposed rule would require that each Covered Company and each bank holding company with consolidated assets over $10 billion (collectively referred to herein as a "Covered Company") establish a risk committee of the board of directors to document, review, and approve, on an enterprise-wide basis, the risk management practices of the company's worldwide operations. RMA generally concurs with the Board about the importance and necessity of requiring the establishment of a risk committee of the board of each Covered Company. However, RMA respectfully suggests that the proper role of the risk committee

should be limited to oversight, and not documentation, of risk management practices. Documentation of risk management practices is clearly within the purview of management of the Covered Company, not the board or a committee of the board.

Structure of the Risk Committee

Section 252.126(a) of the proposed rule sets forth the requirements for membership of the risk committee of the board. RMA agrees with the Board that the risk committee must be chaired by an "independent director," as that term is defined by Regulation S-K promulgated by the Securities and Exchange Commission, must have a formal written charter, and must meet with appropriate frequency, documenting and maintaining records of its proceedings.

The proposed rule would also require the risk committee of the board to have at least one member with risk management expertise that is commensurate with the company's capital structure, risk profile, complexity, activities, size, and other appropriate risk factors. The term "risk management expertise" is defined as (1) an understanding of risk management principles and practices with respect to bank holding companies ...; ***and*** (2) "experience developing and applying risk management practices and procedures, measuring and identifying risks, and monitoring and testing risk controls ...." RMA believes that the use of the word "and" in the foregoing definition instead of the word "or" will result in a shortage of qualified candidates to serve on board risk committees. In short, under the proposed definition, a candidate would be qualified to serve on the risk committee only if he or she understood risk management practices and had served as a chief risk officer of a financial institution. Accordingly, RMA proposes that the term "risk management expertise" be revised to read as follows:

(1) An understanding of risk management principles and practices with respect to bank holding companies or depository institutions, or, if applicable, nonbank financial companies, and the ability to assess the general application of such principles and practices; ***or*** (emphasis added)

(2) Experience developing and applying risk management practices and procedures, measuring and identifying risks, and monitoring and testing risk controls with respect to banking organizations or, if applicable, nonbank financial companies.

Responsibilities of the Risk Committee

It is a fundamental tenet of corporate law that the proper role of the board of directors of an organization is one of policy setting and oversight and not day-to-day management. A director must exercise reasonable care and inform himself or herself of the company's activities and exercise reasonable business judgment based upon that information. The board must delegate the day-to-day routine of conducting the company's business to its officers, but it cannot delegate responsibility for the consequences resulting from unsound or imprudent policies and practices. The proposed rule includes a requirement that the risk committee document, review, and approve the enterprise-wide risk management practices of the company.

While it is within the policy-making and governance powers of a board or any committee thereof to review and approve material corporate policies, the requirement that the risk committee "document, review, and approve the enterprise-wide risk management practices of the company" is not consistent with the proper scope of a board committee. The risk committee should be

charged with oversight of material risk policies, but oversight of risk practices is properly the role of executive management, which should report to the risk committee through the chief risk officer. Accordingly, RMA respectfully suggests that the proposed rule be revised to require the risk committee to review and approve the material enterprise-wide risk management policies of the company, which would include the approval and oversight of the company's risk management framework.

We would generally note that the proposed rule requires the risk committee to manage risk as opposed to oversee policies with respect to risk management. An unintended consequence of this shift in the board's role is to create confusion as to whether particular board actions are properly covered by D&O policies or E&O policies. In cases where the risk committee or the board approves a policy, it is likely that its actions are covered by its D&O insurance. A different result may arise if the risk committee is required to approve the risk management practices of the company. It is unclear whether approval of a practice is within the traditional policy-setting role of the board covered by D&O insurance or is more akin to managing the affairs of the company, which has traditionally been the role served by the officers of the company, who would be covered by E&O insurance. This lack of clarity in terms of coverage may have the unintended consequence of discouraging qualified persons from serving on the risk committee of a Covered Company.

RMA supports the proposed rule requiring the formation of risk committees for Covered Companies, subject to the emphasis on their function as being risk policy oversight as opposed to the management of risk. This would be consistent with the traditional view that boards and their committees are charged with policy setting and review and not implementation or management. RMA recognizes that, while it is important for the risk committee to be independent, flexibility should be preserved at the corporate level if the Covered Company wishes to combine or allocate certain tasks among the risk committee and the audit or other appropriate committee(s) of the board to avoid duplication of risk management oversight functions, and, more importantly, to avoid creating silos among board committees that result in gaps between committees. RMA suggests that while it is appropriate to mandate the formation of a risk committee, the Board should permit Covered Companies to have the flexibility to implement such committees consistent with the respective company's risk profile, complexity, activities, size, and other factors as the board determines from time to time.

Moreover, RMA suggests that the responsibilities of a Covered Company's risk committee should be determined by the board and could include, for example: (a) oversight of the risk management infrastructure, including knowledge of the people, processes, and technology related to the identification, measurement, monitoring, and managing of risk; (b) knowledge of the most significant risks facing the organization and how the organization will respond to a crisis; (c) assisting in the development, communication, and monitoring of the organization's risk tolerance and appetite; (d) simultaneously considering business strategy and risk-taking; (e) oversight of and support for the CRO, for example, through a high-level review of the budget and staffing to ensure adequate resourcing; (f) consultation with external experts to stay abreast of leading practices and new risks, and to benchmark practices and performance; (g) ensuring that an appropriate culture and tone is in place at the top of the organization and is communicated clearly and often throughout the organization; (h) transparent communication of risk to the organization, shareholders, the community, and the investment world; and (i) engaging in continuing risk education, a portion of which is sourced from external resources.

Responsibilities of the Chief Risk Officer

RMA supports the appointment of a chief risk officer by Covered Companies. However, RMA believes that the language used in the proposed rule, namely, that the CRO have "risk management expertise commensurate with the company's capital structure, risk profile, complexity, activities, size, and other risk-related factors" is too subjective a standard and could lead to disagreements between the Board and a Covered Company as to whether a particular candidate for a CRO position meets the requirements for the job. It is unclear whether the standard set forth in the proposed rule will be applied prospectively or retroactively to existing CROs of Covered Companies. Moreover, RMA believes that the prescriptive nature of the proposed rule would unnecessarily limit the pool of qualified candidates for a CRO role. Accordingly, RMA suggests that the Board revise the proposed rule to (a) state that its application will be prospective, not retroactive; and (b) state that the CRO possess expertise commensurate with such factors deemed appropriate by a Covered Company. RMA believes that the CEO and the board should concur that the CRO has the requisite expertise and/or experience to oversee the risk management functions of the Covered Company.

While RMA supports a structure in which, at minimum, the CRO has a reporting relationship to the CEO and to the board risk committee, we do not believe the CRO should be subject to a ***mandatory*** dual-reporting requirement. The board and management should have sufficient flexibility to determine the structure that best suits their institution, based on the culture, business strategy, and risk profile of the institution and the skill and experience of the CRO.

The CRO cannot solely manage all risks, but is part of a framework that inextricably links several risk resources in the institution. The requirement that the CRO "directly" oversee all functions fails to acknowledge that he or she works with, and through, the business units and staff functions in the institution. Individual business units within an institution have a primary role in risk management, including identifying risks and monitoring risk exposures. The business units are most closely involved in the day-to-day operations of the company and must translate risk management policies into operational practices and procedures. The CRO should have a sufficient degree of autonomy from the business units, but sufficient authority within the institution to oversee the risk decisions of the business units and be able to effectively challenge risk decisions that affect the business units.

Sincerely,

William F. Githens

William F. Githens