27 March 2012

Ms Jennifer J. Johnson
Secretary
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue, NW
Washington, DC 20551

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

Dear Ms Johnson,

Thank you for the opportunity to comment on the proposed rule "Enhanced Prudential Standards and Early Remediation Requirements for Covered Companies," published in the Federal Register, vol. 77, no. 3, on January 5, 2012. We would like to respond to questions 62 to 67 regarding "Risk Management and Risk Committee Requirements" and questions 68-69 applying to "Appointment of CRO."

These comments are derived from two sources. First, from experience and analyses across risk management disciplines (strategy, financial, financial engineering, operational (e.g., business continuity, process improvement, quality control, information technology, security and project), industries and countries. The analyses on operational risk were compiled into The Operational Risk Handbook for Financial Companies (Harriman House, London, 2011). Second, from analyses for the recent white paper "Two years after the SEC mandated disclosure on Board Oversight of Risk, what insight have investors gained? Not Enough. A review of disclosures required by the U.S. SEC Proxy Disclosure Enhancement rule provision on Board Role in Risk Oversight."

In responding to all questions, four points are in common:

- A key aspect in the quality of risk oversight and management is the diversity of board member professional, industry and country experience to understand the range of risks to the range of business activities (products and processes).
  - This diversity of skill is required in most any team seeking to accomplish an objective from a sports team to transportation accident investigation team to leaders of a new venture company.
  - The "surprise" of financial company leaders to company-wide, operational and systemic risks that are common in other areas (professional disciplines, industries or countries) has made gaps in this range of experience this painfully obvious.
  - The financial community tends to regard risk as something to model; that is it regards probabilities as more or less knowable. This contributes to systemic risk when best estimates prove wrong by orders of magnitude. Another effect of this view of risk is to

disregard ambiguity, or what academicians call Knightian uncertainty, in risk planning. Knightian uncertainty states that there is a limit to risk planning, since the world changes in unpredictable ways, changing the risk parameters. This, in turn, would call for an emphasis on robust and flexible ability to respond, rather than risk identification and the false precision of modeling, something that is more common in operational companies rather than the financial community where highly levered balance sheets contribute to fragility, not robust capacity.

- That real risks to institutions and economies in the real world will only be sufficiently addressed when institutions (and regulators) more fully shift their view of risk management (especially company-wide and operational) to more *prospective management of risk to business performance objectives* (financial and operational), from one of retrospective compliance reviews.
    - Entities that were compliant, yet suffered injury occur repeatedly in areas ranging from data breach to trading losses to industrial injuries.
    - Fostering real risk management, not just checking compliance, is the emphasis.
- A wasteful consequence of compliance-driven risk management has been churn around how compliance processes work, instead of emphasis on understanding of how the products and processes of complex and changing activities in a bank actually work, especially in an even more complex and changing world.
    - For example, most successful frauds are about the perpetrator knowing the victim's processes better than the victim does. In the extreme, after 9/11, financial regulators were shocked to learn about the communications infrastructure dependencies in lower Manhattan. Yet, the Federal Communications Commission was not only aware, but also engaged in detailed rule making about the prices charged by one carrier to another for those network elements.
    - Thus, the first imperative is to more fully *know the business*.
- With increased knowledge of the external environment and internal capabilities, and freed from the wasteful diversion of resources on compliance-driven approaches to risk management, institutions can focus on creating robust, yet simple approaches to risk management.
    - "Simple" in the sense the process is widely understood and efficient enough to be embedded into daily decision-making from the boardroom to the front lines. This includes, clear common language, freed from the jargon and buzz-words that sadly complicate risk management today, including across business lines and functions within an institution. The BCBS and EU documents especially struggle with this, leading to further complications for banks operating in multiple jurisdictions and languages. By contrast, the US Federal Emergency Management Agency requires common language for emergency responders for more effective action. Similarly, the Board, in conjunction with global regulators, ought to spearhead a move towards clear, common language reporting of risks to performance objectives.

These four points are critical to improving confidence in risk oversight and management that is needed by all those with a stake in the financial system and global growth.

VI. Risk Management
B. Overview of the Proposed Rule
1. Risk Committee Requirements
a. Structure of Risk Committee (Section 252.126(b) of the proposed rule)

Question 62: Would it be appropriate for the Board to require the membership of a risk committee to include more than one independent director under certain circumstances? If so, what factors should the Board consider in establishing these requirements?

> Response: Yes. Drawing on the four common points above, as bank managers and inside directors are more likely to have insular careers within financial services, it is especially important to have diversity of experience (in risk-related professional backgrounds and industries) on board risk committees. Thus, the suggestion is for a rule that would: 1) require independent directors on risk committees in a ratio no less than the total board (rounded up to the nearest full person); 2) recommend (but not require) at least half independent directors; and 3) the examination criteria be that the committee reflects experience across types of risk within a bank, professional disciplines and industries.

Question 63: Should the Board consider specifying by regulation the minimum qualifications, including educational attainment and professional experience, for risk management expertise on a risk committee?

> Response: Yes, but only with regard to professional experience. Drawing on the four points above, the critical need is for diversity of experience across professional discipline backgrounds and industries so that board members individually and collectively can draw on a greater sense of "been there, done that" in asking "what if?" regarding how situations can unfold given an external environment and internal capabilities, and warning signs. Regarding type or level of expertise:
>
> - The proposed rule focuses on "risk management expertise that is commensurate with the company's capital structure, risk profile, complexity, activities, size, and other appropriate risk-related factors."
> - This long list tends to distract from the central factors – capital structure (driving financial and some strategic risks) and activities (served markets, products, processes, mergers and acquisitions, and related). Complexity and change in capital structure and activities are the practical drivers of the real risks. Risk profile is merely record-keeping for the real drivers and size is a loose proxy for risk. Thus, would simplify to eliminate the "apples and oranges" sense to the list and improve focus on the key drivers of risk.
>
> Regarding specific education:
>
> - It is less important that one member have deep expertise in what is often excessively complicated risk management processes and jargon (as noted above, too often taught in

the financial services industry in a silo and complicated way that precludes efficient and effective daily risk-aware decision making) than that all board members have a working knowledge of a robust, yet simple risk management process. This clarity will enable members to both exercise oversight of management's risk-aware decisions and demonstrate this behavior for the institution as board members who make their own risk-aware decisions. This said, it is indeed helpful for one member to have depth in multiple, formal approaches to risk management so that s/he can deeply critique management's approaches and avoid systematic errors in business decisions because of systematic errors in risk management processes. That person could also drive board evaluation and training, starting with his/her own ongoing education.

- The suggested evaluation criteria in both cases are discussions with both the designated risk management leader and all board members to allow each board member to describe their depth of understanding of risks to the bank and how they apply their personal risk management experiences to the needs of the bank. Moreover, as risk is an ever-changing discipline and knowledge advances in fits and spurts, it is far too easy to become static; the chairman of the Risk Committee should be required to affirmatively state that the Committee has a) reviewed the institution's risk management policies and processes at least annually. The Board should further consider whether to mandate a continuing education requirement for members of the risk committee.

Question 64: What alternatives to the requirements for the structure of the risk committee and related requirements should the Board consider?

Response: The strength of a specific risk committee is that it provides focus. The weakness is that it may create a feeling of "someone else's" job by board members not on the risk committee. Again, drawing on the four initial points, if a key is diversity of experience to oversee the process for evaluating the range of risks to the range of business activities, then it quickly becomes clear that "risk is everyone's job." In this case, the risk committee charter should include responsibility for overseeing the specifics of management's process and that risk is adequately reflected in the board's own activities. These board activities include: a) the board's own decision-making b) relevant risks being addressed in each committee, and c) evaluation, selection and training of board members. Due to differing committee structures and maturing board members, is it suggested that examination criteria provide for latitude in approaches used to achieve the objective.

b. Responsibilities of Risk Committee (Section 252.126(c) of the proposed rule)

Question 65: What is the appropriate role of the members of the risk committee in overseeing enterprise wide risk management practices at the company and is that role effectively addressed by this proposal?

Response:

First, it is suggested that the risk committee address each of the critical areas described in the response to Question 64.

Second, the board, and each committee as appropriate, implement the fundamental four functions of a governor. In the context of risk management, they are summarized as:

- Setting an example of risk-return aware decision-making through the board's own decisions
- Improving the culture at all levels (by both example and oversight)
- Ensuring integration across all types of risk management
- Evaluating management's implementation of risk management

Third, that the board and risk committee drive continual improvement within both the boardroom and management, by drawing on recognized guidance from organizations such as the International Corporate Governance Network (ICGN), as well as regulators.

Question 66: Is the scope of review of enterprise-wide risk management that this proposal would require appropriate for a committee of the board of directors? Why or why not?

Response:

Within the context of the responses to Questions 64 and 65, generally yes.

However, the proposed rule's excursion into the elements of a "framework" is weak and potentially hazardous to efficient and effective risk management by enshrining awkward notions that do not reflect lessons learned in risk management from across professional disciplines, industries and the decades.

- A "framework" generally includes objectives and metrics, processes (with inputs and outputs), structures and roles (with accountabilities), and a method for evaluating both processes and outcomes. This applies to most anything from aviation, to public health to supply chain management. Examples exist elsewhere within federal government (the Coast Guard's performance focused risk management is one example). A comparison of the proposed rules with these aspects quickly shows both gaps and excesses.
    - A suggested alternative is "that a company's risk management framework must include: For each business line, financial and operational objectives along with capacity to take risk in pursuit of those objectives, acceptable range in daily activities, and impact of those objectives and ranges on compensation; risk oversight and management processes, structures (including roles and accountabilities) and communications for risk evaluation and response."
    - This alternative provides more focus on key aspects as reflected in decades of proven practice in other industries and disciplines, including that used elsewhere in federal government. It also simplifies the Board's future efforts as it provides a broader range of proven experience from federal government and private industry on which the Board can draw.
- Two phrases are especially hazardous.

- "Risk control" suggests that risks in the real world are subject to tidy, easy to enforce controls. Real world experience shows "controls" are a) confusing to apply because of multiple definitions and b) few strategic, market or operational risks are neatly "controlled." Even if trading positions were as tightly controlled as pharmaceutical manufacturing a) market forces aren't and b) drug recalls still happen. "Risk controls," while potentially appropriate for financial reporting are totally inappropriate for the realities of risk causes in the real world. Thus, "risk controls" can dangerously distract institutions from: a) evaluating the range of risks to the range of business activities (rather than just those that are deemed "controllable" as so often wastefully occurs) and b) apply a range of responses to risk (governance, management, controls, and core business process improvements) to improve an institution's position in the environment or strengthen capabilities. If emphasis is placed on any particular action, a more productive area would be board reviews of the quality of "Plan B's." Drawing on experience from elsewhere in the federal government, it might be helpful to consider the way the NTSB recommends the use of back-ups and other responses in commercial aviation to be ready to address the inevitable situations that arise. This Plan B emphasis is also entirely consistent with Basel III's focus on resilience.
- "Emerging risks" suggests that many risks are new to the world – a bit like Columbus "discovering" America or western newspapers rushing to "discover" the gorilla. Too often "emerging risk" lists are used as excuses when situations that are already well known in other areas of an institution, other institutions, other markets or other industries happened to be encountered by an previously uninformed individual.

Question 67: How can the Board ensure that risk committees at companies have sufficient resources to effectively carry out the oversight role described in this proposal?

Response: Under the proposed rule, this is complicated to evaluate because the proposals imply an emphasis on compliance-driven risk management rather than the performance-driven emphasis contained in other language of BCBS and Board documents (especially those related to bank ability to attract capital and deposits, and contribute to economic growth).

By contrast, if the four key points and the prior question responses are accepted, then the evaluation of resources becomes much easier. A committee's effectiveness can be evaluated on both process and outcomes using criteria such as the ICGN Risk Oversight Guidelines and the four functions of a governor from The Operational Risk Handbook. This would enable an examination interview focus on demonstration of sufficient resource by asking: a) how a board has guided management to a robust, simple and deeply used risk management process; and b) the degree to which the board has learned and directed revisions in the process when business outcomes varied from objectives. This is the key need for investors, guarantee funds, customers and all participants in the economy.

2. Additional Enhanced Risk Management Standards for Covered Companies. (From section 165(b)(1)(A)(iii) of the Dodd-Frank Act)

a. Appointment of CRO

Question 68: Should the Board consider specifying by regulation the minimum qualifications, including educational attainment and professional experience, for a CRO? If so, what type of additional experience or education is generally expected in the industry for positions of this importance?

Response: No.

- As discussed with regard to board member experience, an effective senior risk leader (as in other industries and in senior officers in general) benefits from a diversity of professional discipline, country and industry experience.
  - Depending on the maturity gaps and business objectives of a specific company, the needed experience in a CRO may vary over time.
  - The CRO need not be a functional specialist, although it is more likely in a smaller company.
  - As a practical matter, there is no one academic or professional education program that captures the diversity of helpful professional experience for the simple reason that academic departments and professional associations by necessity target specific audiences with slices of education. If the Board is interested in reviewing more cross-discipline guidance, in the governance and risk space, the most appropriate organization is probably OCEG (www.oceg.org).
  - As noted earlier, the need is for a) knowing the business and b) driving a robust, yet simple process that is deeply embedded and used in daily decision-making. Thus, a desirable career path may be for a leader who has experience in operations, finance and leading a smaller business line to then become CRO, and from there take a more senior role in another function, geographic unit or larger business line. If properly supported by the board, this approach can be a lever to more deeply ingraining risk-return aware decision-making into daily business.
- To the extent to which the Board wishes to evaluate the potential contribution of a CRO to improving the risk management process and business outcomes, the above considerations can be used in a discussion with a CRO and feedback to the board's chair and/or designated risk management expert.

Question 69: What alternative approaches to implementing the risk committee requirements established pursuant to the Dodd-Frank Act should the Board consider?

Response: Please see the four key points and responses to prior questions.

Respectfully submitted,

Jon Lukomnik
Managing Partner
Sinclair Capital, LLC

Brian Barnier
Principal
ValueBridge Advisors, LLC