Paul J. Sobel, CIA, CRMA
Chairman of the Board
Institute of Internal Auditors
247 Maitland Avenue
Altamonte Springs, FL 32701
United States of America

30 September 2013

Mr. Svein Andresen
Secretary General
Financial Stability Board
Bank of International Settlements
Centralbahnplatz 2
CH-4002
Switzerland

Dear Mr. Andresen,

RE: FSB Principles for an Effective Risk Appetite Framework Consultation Draft

On behalf of the over 180,000 global members of The Institute of Internal Auditors (The IIA), I am pleased to provide our observations and comments on the Financial Stability Board's (FSB) Principles for An Effective Risk Appetite Framework Consultation Draft. As the global standards-setting body for the professional practice of internal auditing, we appreciate the opportunity to provide comment on these principles for an effective risk appetite framework (RAF) and fully concur with the concept that an RAF forms the foundation of good risk management.

As noted in the FSB's February, 2013 Thematic Review on Risk Governance Peer Review Report, "assessing a firm's RAF is a challenging task that requires greater clarity and an elevated level of consistency… at the core of the RAF is firm's RAS (risk appetite statement)…" We completely agree; a well crafted, fully-vetted RAS should become the strategic underpinning supporting a firm's risk management framework, organizational governance and even its culture.

The IIA applauds the efforts of the FSB in proposing a principles-based RAF that sets minimum expectations and establishes common nomenclature for systemically important financial institutions (SIFIs), and other firms. Our comments are based on discussions conducted by a core team of globally represented internal audit professionals who are thought leaders with experience in the public and private sectors; internal and external auditing; and small, medium, and large domestic and multinational companies, both within and outside of the financial services sector.

Our primary comments related to the Consultation Draft are below. Additional, more detailed observations and comments are provided in Attachment A.

Overall the framework has been well thought out and offers a good balance of high level principle-based guidance with enough detail to provide direction. We believe, however, that there remain opportunities for further consideration. Principally,

1) The concepts and principles embedded in a strong, progressive and effective RAF have applicability beyond SIFIs and, for that matter, beyond financial services firms in general, so due care in promulgating guidance as it relates to such critical matters should continue to be exercised.

Global Headquarters
247 Maitland Avenue
Altamonte Springs, FL
32701-4201 USA
T: +1-407-937-1100
F: +1-407-937-1101
www.theiia.org

2) The consultation document outlines definitions for many of the key concepts and terms used within (e.g., risk appetite framework, risk capacity, risk appetite, etc.). These definitions are useful in the context of this framework, but can be confusing when these same or similar terms have been defined through other globally recognized means. An example where such terms are defined is ISO Guide 73. Ensuring clarity among terms and, as expressly desired, establishing a common nomenclature, can be a challenging task.

3) When dealing with risk, the concept of materiality becomes critical. The consultation document refers to "material risk" in a number of places, yet does not provide guidance as to what constitutes material risk and/or what criteria should be considered when evaluating materiality in relation to the establishment of a RAF. Further guidance, either by incorporation or reference, would be helpful in this regard.

4) How an effective RAF takes into consideration the ways risk manifests itself, whether though financial, market, credit, operational, as well as other factors, can be difficult. The consultation draft could be greatly enhanced, either directly or through reference, by providing guidance to organizations as to how to navigate the full range of risks when deliberating its RAF and consequent risk appetite statement.

5) We believe that a robust RAF is a key overarching element of an Enterprise Risk Management (ERM) process. Guidance on how the RAF is incorporated into an organization's broader ERM framework would be helpful.

6) The consultation draft introduces that "an appropriate RAF should enable risk capacity, risk appetite, risk limits, and risk profile to be considered at the legal entity level as well as within the group context." This terminology is causing concern amongst many organizations that have very complex organizational structures, whereby they may have hundreds of "legal entities," but that may not be the way they manage risk. Complex organizations often begin considering risk at the enterprise level. Then, from there, they establish risk management capabilities at both the enterprise and business line level, potentially regardless of a legal entity context. We would propose that the FSB reconsider the "legal entity" construct, especially as it relates to SIFI's and their potentially complex legal entity structures that may not be consistent with how they actually manage the institution and its attendant risks.

7) Lastly, while very likely not intended as part of this consultation draft, many practitioners will be looking for concrete examples and even potentially an implementation guide. If the FSB does not have plans to promulgate such additional guidance in the future, it should encourage others to do such in order to provide organizations and practitioners direction in the mutual pursuit of effective organizational risk management.

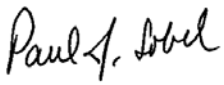
We are pleased to see the inclusion of the valuable role of internal audit in providing assurance on the RAF on a firm-wide and individual business line basis. Certified Internal Auditors (CIAs) and holders of the Certification in Risk Management Assurance (CRMA) are very capable of providing this assurance and The IIA will continue to provide guidance to CIAs, CRMAs and other internal auditing professionals to as they fulfill their assurance responsibilities.

The IIA is the global leader, chief advocate and, as mentioned previously, the standard-setting body for internal auditing professionals serving financial institutions as well as entities within the private and public sectors. We are committed to enhancing the global profile of, and demand for, professional internal auditing and building awareness on the critical role of internal auditing in good organizational governance, risk management and control.

Please do not hesitate to contact Stacy Mantzaris, IIA's Director of Global Advocacy, if you have any questions about this response and/or would like to schedule a time for us to either meet in person or via conference call. Ms. Mantzaris can be reached via email: stacy.mantzaris@theiia.org or phone 1.407.037.1290.

Again we applaud the efforts of the FSB to promulgate principles for a RAF designed to advance good risk management practices. We welcome an opportunity to meet with you to not only discuss our comments, but to explore other collaboration opportunities in furtherance of our respective missions.

Best Regards,



Paul J. Sobel, CIA, CRMA
Chairman of the Board

Attachment A
Specific Recommendations/Comments

Section	Recommendations/Comments
II. KEY DEFINITIONS	
• Risk Appetite Statement: As currently worded this definition combines generalities and specifics. Rather, we suggest generalizing risks into the categories of, for instance, reputation, fraud and unethical practices vs. "reputation and money laundering and financing of terrorism risk, as well as business ethics and conduct". We also suggest adding social and environmental risks. For example: "reputation, fraud, unethical practices, social and environmental risks..." • Risk Tolerance is a term often used in risk management and warrants either a separate definition or further explanation as to the rationale for its exclusion as noted footnote 3.	
III. PRINCIPLES	
1. Risk Appetite Framework	Next to last sentence, first paragraph: Suggest adding "business line" within the legal entity and group context: For example: "The RAF should enable risk capacity, risk appetite, risk limits, and risk profile to be considered at the legal entity and/or business line level as well as within the group context." Last sentence, first paragraph: This sentence implies a conclusion from the previous sentence(s) by starting with "as such". However; the logic does not seem to flow in relating an RAF to the development of IT and MIS. This should be explained further or clarified.
	1.1 An effective RAF should: Item (c) – For clarity purposes we suggest rewording this statement to read "facilitate embedding risk appetite thinking into the firm's ~~risk~~ culture." Item (d) - It is not clear how a RAF would "act as a brake against excessive risk-taking." However it is clear that the RAF can act as one, albeit strong, defense against excessive risk-taking. Suggest substituting term "defense" (or something similar) for "brake." Item (e) – Suggest modifying last part of statement to read "…can effectively and objectively assess and evaluate ~~credibly debate and evaluate~~ management recommendations and decisions in a risk-based context." Suggest adding Item (h) – "Cover activities, operations and systems of the firm that fall within its risk landscape but are outside its direct control, including subsidiaries and third party outsourcing suppliers."
2. Risk Appetite Statement	**2.1 Key elements of a risk appetite statement should:** Suggest rewording of this sub-head for 2.1 to read "An effective risk appetite statement will:" as this seems to be more about the elements of what would make a risk appetite statement most effective and using "will" sets the minimum parameters of an effective risk appetite statement. Item (e) – We clearly understand the difficulty in measuring certain risk consequences, with reputation being a good example. However, we were confused by the phrase "poor management of conduct risks" that followed. We believe this needs further clarity.
3. Risk Limits	See previous reference above to the term "brake." We propose using a different term, such as "defense".

Section	Recommendations/Comments
4. Roles and Responsibilities	In order to provide additional clarification of the roles and responsibilities of the board as an oversight function versus the management function, we suggest incorporating the following statement from footnote 6 into the main body of the document: "Recognizing that different structural approaches to corporate governance exist across countries, this document encourages practices that can strengthen checks and balances and sound risk governance under diverse structures." The first sentence begins, "The board of directors must establish..." Technically, we view it that the board of directors does not "establish" anything in particular. However, the board should approve the RAF and should provide oversight to ensure conformance with it. As well, in the first sentence, we suggest adding "among others" to the articulated roles of CEO, CRO and CFO. (We believe this should be done throughout the document, as in 4.2, 4.3, 4.4, and 4.5, where specific roles are identified, as organizations may have different organizational titles, as well as have additional organizational parties, like a COO or Chief Audit Executive (CAE) involved.) In the third sentence of the first paragraph, for further clarification we suggest replacing the concept of "maintenance of controls" with the concept of "ongoing monitoring and evaluation of controls". As a result, we suggest having the sentence read "...ongoing monitoring and evaluation of the design and overall effectiveness of a firm's internal controls..."
	4.1 The board of directors should: (g) Suggest incorporating materiality into the statement, such as: "question senior management regarding any material activities….."
	4.6 Internal audit (or other independent assessor) should: (a) Suggest removing "routinely," keeping the statement at a high level and more principles based. Internal audit (or other independent assessor) should definitely "include assessments of the RAF …", but the periodicity of the assessment should be left to the experience and judgment of the internal auditor (or independent assessor). (c) Requires internal audit to "assess at least annually the design and effectiveness of the RAF." Annually may be too frequent for a comprehensive assessment of the design of the RAF, which is unlikely to dramatically change each year. In order to remain high level and principles based, we suggest not specifying a time frame but using the term "regularly" as stated in other areas throughout the document, allowing for the exercise of judgement by the independent assessor as to the frequency. (d) Since internal audit plays an essential role in assuring the board about the risk and control culture, this statement should address assuring that the tone set at the top, or culture, related to risk is properly reflected at all levels of the organization. Suggest revising to: "assess the effectiveness of the implementation of the RAF, including linkage to organizational culture, as well as strategic and business planning, compensation, and decision-making processes." (e) Consider changing the language from "validate" to "evaluate the design and effectiveness of …" Validation is a confirmatory term and should be the role of management not internal audit. Internal audit can evaluate and report on the design and effectiveness of risk measure techniques, etc. (f) Modify to address the concept of materiality by stating "report any material deficiencies in the RAF…" Also, we suggest that language be added to introduce the concept that internal audit (or the independent assessor) consider not only the materiality of deficiencies in isolation, but should also evaluate the materiality of deficiencies when considered in the aggregate. Suggest adding item (h) - In order to remain high level and principles based, we suggest adding a further statement: "To ensure effectiveness, internal audit (or other independent assessor) should conduct its work in conformance with a set of widely accepted professional standards, such as The Institute of Internal Auditors *International Standards for the Professional Practice of Internal Auditing (The Standards).*"