Andrés Portilla
Director, Regulatory Affairs Department

September 30, 2013

Mr. Svein Andresen
Secretary General
Financial Stability Board
Bank for International Settlements
Centralbahnplatz 2
CH-4002 Basel Switzerland
Submit via email to: fsb@bis.org

RE: IIF Response to FSB's *Principles for Effective Risk Appetite Framework*

Dear Mr. Andresen:

The Institute appreciates the opportunity to comment on the proposed FSB Principles ("*Principles")*. Since 2008, the Institute has devoted substantial effort on industry practices, in particular in the areas of risk management and risk governance.[1] These efforts are complemented by industry surveys to assess how much progress the industry has made in revamping its practices. [2] These surveys have shown that the industry has made significant progress, but at the same time have recognized the need for further improvements in some areas of banks' risk practices. Hence, the release of the FSB's *Principles for Effective Risk Appetite Framework ("Principles")* provides further opportunity to extend the discussion on risk appetite frameworks, their development, and implementation. In fact, in broad terms, there is a great deal of alignment between the FSB *Principles* and a number of concepts that the Institute has discussed in its reports, *Implementing Robust Risk Appetite Frameworks to Strengthen Financial Institutions* (June 2011) and *Governance for Strengthened Risk Management* (October 2012).

The Institute hopes that as institutions continue to develop more robust risk appetite frameworks, there will be effective ongoing dialogue with supervisors in order to foster an improved, mutual understanding of the arrangements that contribute to effective risk governance in light of institutions' different governance structures and business models, and also foster a better understanding of supervisory expectations with regard to the design and implementation of risk appetite frameworks. It is anticipated that such continued dialogue

[1] IIF, *Final Report of the IIF Committee on Market Best Practices: Principles of Conduct and Best Practice Recommendations,* July 2008; IIF, *Reform in the Financial Services Industry: Strengthening Practices for a More Stable System,* December 2009; IIF and McKinsey&Co, *Risk IT and Operations: Strengthening Capabilities,* June 2011; IIF, *Implementing Robust Risk Appetite Frameworks to Strengthen Financial Institutions,* June 2011; and IIF, *Governance for Strengthened Risk Management*, October, 2012.
[2] IIF and Ernst&Young, *Risk Governance – Agenda for Change: Survey of the Implementation of the IIF's Best Practice Recommendations,* December 2009 (an appendix to the report on *Reform in the Financial Services Industry*); IIF and Ernst&Young, *Making Strides in Financial Services Risk Management,* 2011; IIF and Ernst&Young, *Progress in Financial Services Risk Management: A Survey of Major Financial Institutions,* 2012; and IIF and Ernst&Young, *Remaking Financial Services: Risk Management Five Years After the Crisis – A Survey of Major Financial Institutions,* 2013.

may help to clarify where appropriate degrees of flexibility may be brought to bear in the practical application of the *Principles,* particularly with respect to roles and responsibilities of the various functions, which the Institute hopes will take into account varying organizational differences.

The Institute's response below first addresses general points of emphasis, and then turns to specific areas in individual sections of the *Principles,* including comments on issues where clarification may be needed in order to minimize implementation challenges.

1. General Comments

Alignment of RAF with business planning processes

The *Principles* clearly articulate an important role of the RAF within the firm's strategy and business planning processes. While the industry appreciates this and recognizes that the FSB intends firms to have RAFs that can be distinctly identified apart from their business strategies, some of the wording[3] could be interpreted as though the RAF should be considered independently from business strategy and capital planning.

The Institute is of the view that the RAF should be aligned with the business plan, strategy development, and capital planning of an institution. As noted in the report, *Implementing Robust Risk Appetite Frameworks to Strengthen Financial Institutions,* "The establishment of an effective link between the risk appetite framework and the strategy and business planning processes is fundamental."[4] This is not to say that the RAF should be solely led by the business planning process. The RAF should have continuity and stability – standing on its own merits; however, it should be aligned with the planning processes. In this context, although each institution may take a different approach depending on internal processes and procedures, the Institute has noted a trend where boards increasingly tend to review and approve the business strategy, capital management plans (including the Internal Capital Adequacy Assessment Process), and the risk appetite statement at the same time, in order to maintain such alignment. An emphasis on this point of alignment will be very helpful in providing clarity about the link between the RAF and business planning.

The iterative nature of developing the RAF

The Institute has consistently held that the development of a robust RAF is a time-consuming, iterative process that requires ongoing dialogue throughout the firm.[5] During the course of its development, the RAF goes through an evolutionary process as it is built, modified, developed, added to, and subtracted from. This iterative, evolutionary process is essential, because risk appetite is a complex and relatively new concept in many institutions,

---

[3] For example, the opening of the RAF Principles section says, "The RAF sets the firm's risk profile in the course of implementation of the firm's strategy and the risks undertaken in relation to the firm's risk capacity. For the purpose of these Principles, the RAF does not include the processes to establish the strategy, develop the business plan, and the models and systems to measure and aggregate risk." (*Principles,* Pg. 3).

[4] IIF, *Implementing Robust Risk Appetite Frameworks to Strengthen Financial Institutions,* June 2011. Pg. 29 (and IIF, *Governance for Strengthened Risk Management* of October 2012 (Pages 4 and 20) also emphasize this point).

[5] IIF, *Implementing Robust Risk Appetite Frameworks to Strengthen Financial Institutions,* June 2011. Pg. 11

and experience in leading institutions to date has shown that it takes some time to develop a true consensus among all stakeholders regarding the desired placement, articulation and refinement of the boundaries of risk appetite, and a large amount of "learning by doing" is required in order to ensure that the risk appetite is expressed in a manner that is helpful for guiding day-to-day business. Although time-consuming, this process is extremely valuable and also enables the institution to attain crucial buy-in from the different business units.

The *Principles* mentions the iterative process once, in the context of assessing "a firm's consolidated risk profile against its risk appetite."[6] Although this acknowledgement is helpful, it does not address the overall iterative and evolutionary nature of the RAF development. It may be that this is implied in the *Principles*; however, we think that this could be further emphasized as firms continue to establish robust RAFs, and in particular, as ongoing discussions are carried out with supervisors through the RAF development process.

Application of RAF to business lines vs. legal entities

The *Principles* seem to imply strongly, from the outset, that the RAF and its derived components, such as risk appetite statement, risk limits, and risk capacity should always be applied without a measure of *proportionality*, at the legal entity level, regardless of the *materiality* of the legal entity's operations.[7] If literally applied, this concept would create a significant challenge for institutions with numerous legal entities, many of which are not material from the group-wide perspective. In addition, application of the RAF at the legal entity level ignores the fact that most institutions are risk managed on a business line basis. (The detailed *Principles* do mention application by business lines, but the introduction to the *Principles* neglects to mention this, potentially creating confusion). We believe the RAF should ideally be established on a group-wide basis, and subsequently proportionally cascaded down to business lines AND/OR legal entities on the basis of relevance/materiality to the group's overall operations. In certain cases, where the materiality of the risks engendered by a business line or legal entity is minimal, applying other alternative risk management tools (e.g., risk limits) instead of a full blown RAF may suffice as a proportional application of risk governance measures.

This overarching issue is discussed further in the specific comments below, under the *Risk Limits* sub-section.

Importance of risk culture in the RAF process

Although the *Principles* recognize that an effective RAF will help reinforce a strong risk culture in an institution,[8] the Institute would emphasize that a good risk culture is also

[6] *Principles,* Pg. 3
[7] The *Principles* states, "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." Pg. 1
[8] The *Principles* notes, "Establishing an effective RAF helps to reinforce a strong risk culture at financial institutions, which in turn is critical to sound risk management" (Pg. 1).

fundamental to the development of an effective RAF.[9] Some have argued that it is very difficult to develop an effective RAF without a strong risk culture already in place. Hence, risk culture and risk appetite are considered to be inextricably linked and mutually reinforcing concepts that help foster an effective overall risk governance framework. This is rather a point of emphasis, as it is clear that the FSB shares the view that a "sound risk culture will provide an environment that is conducive to ensuring that emerging risks that will have material impact on a firm, and any risk-taking activities beyond the firm's risk appetite, are recognized, escalated, and addressed in a timely manner."[10]

Developing a strong risk culture is a complex undertaking that involves aligning the behavior of individuals with the firm's attitude to risk taking and risk management.[11] It is largely behavioral and thus difficult to embed and measure. Consequently, developing a good risk culture is an element in the risk governance process that also takes time to foster (similar to the development of a RAF), because it requires buy-in from various stakeholders (besides the risk function) within the institution. However, the recent IIF-EY survey shows that firms are giving high priority to improvement of risk culture. Such efforts will lead to the appropriate environments for developing increasingly effective RAFs.

Recognition of different governance structures and business models

As indicated above, the *Principles'* provisions related to specific roles and responsibilities of the board and the senior management of institutions seem too prescriptive in certain areas. The Institute would note that although all organizations must address the risk management requirements identified in the *Principles*, different organizations may vest certain board responsibilities with board committees or certain senior management functions in different senior executives or their delegates. Instead of prescribing specific functions to be performed by boards of directors or specific senior officers, the *Principles* should identify functions for which the board or senior management would be responsible, and then permit firms to allocate these functions, in light of each firm's specific organization and risk profile. As recognized at the outset of the consultative document, "The FSB Principles are high level to allow financial institutions to develop an effective RAF that is firm-specific and reflects its business model and organization…"[12] This view should similarly apply to the roles and responsibilities section. Additional comments about the roles and responsibilities of the board and senior management would be made further below.

2. Specific Comments

Definitions

The key terms defined in the *Principles*: risk appetite framework, risk appetite statement, risk appetite, risk capacity, risk profile, and risk limits, are generally in alignment with the Institute's views on these terms. With respect to ***risk capacity*** and ***risk profile***, the

[9] IIF, *Implementing Robust Risk Appetite Frameworks to Strengthen Financial Institutions,* June 2011. Pg. 11
[10] *Principles,* Pg. 1
[11] IIF, *Governance for Strengthened Risk Management,* October 2012. Pg. 1.
[12] *Principles*, Pg. 1

Institute would like to provide further input to enhance and stress certain aspects of these key terms.

The definition of *risk capacity* seems overly narrow. It refers to the maximum level of risk the firm can assume, before breaching constraints, that is determined by regulatory capital and liquidity needs.[13] The Institute recognizes that in some cases there are other very important, wider constraints on risk capacity, such as limitations on the firm's risk management capabilities or expertise in particular areas (including the ability to understand, measure and effectively manage the risks associated with particular products, the quality and robustness of the firm's risk data and IT infrastructure, including its risk aggregation capabilities etc.), earnings capacity (although shareholders are mentioned, the point is not fully captured) and other considerations related to the operational environment that would contribute to defining an institution's risk capacity. These additional constraints may be implied by some of the language in the text: "…obligations, also from a conduct perspective..."[14] However, additional clarity on this will be helpful. Frequently, these considerations are actually binding on the risk capacity of individual firms in particular products or business lines. The IIF report, *Reforms in the Financial Services Industry* also indicates that "borrowing capacity, and regulatory constraints are all components of a firm's risk capacity."[15] Risk capacity is very fundamental to management's understanding of the total view of the nature of risk that a firm can assume. Hence, we believe a wider definition that encompasses these considerations in addition to regulatory capital and liquidity coverage would be more appropriate.

With regard to *risk profile*, the *Principles* state that it is the "point in time assessment of the firm's net risk exposures (after taking into account mitigants) aggregated within and across each relevant risk category based on forward looking assumptions."[16] The Institute would suggest that a firm's risk profile is composed of both its gross risk exposures and the resulting net risk exposure after mitigants are considered. The emphasis on "net risk exposures" seems to indicate that the risk appetite statement will always be on a net basis. This will, in some cases, be unlikely because a net computation depends on the kind of risk category that is being referenced. Hence, a definition of risk profile that would say, "point in time assessment of the firm's ~~net~~ *gross and net* risk exposure, (after taking into account mitigants)…" would be preferable and would take into account all aspects of risks. Essentially, there are instances where exposures need to be reviewed on a net and gross basis and with appropriate reference to any basis risks associated with net exposure.

Finally, footnote 3 explains that the *Principles* exclude the definition of "risk tolerance" from the list of definitions because the term is sometimes used (along with "risk appetite" and "risk limits") by different authors with slightly different meanings. However, while we do not disagree with the decision not to define this term, we would note that a number of institutions find the term risk tolerance useful to describe risks such as operational and reputational where the term "risk appetite" would possibly provide the wrong connotation. Furthermore, for certain organizations, such as insurance institutions, risk tolerance is an important term used to broadly identify overall amount of risk a firm is

[13] *Principles,* Pg. 2
[14] Ibid
[15] IIF, *Reform in the Financial Services Industry: Strengthening Practices for a More Stable System,* December 2009
[16] Ibid.

willing to accept within certain constraints, similar to the definition of risk capacity. Hence, the use of the term "risk tolerance" is useful in particular instances and the FSB should emphasize that its exclusion in the list of definitions does not preclude firms from using it.

Risk Appetite Frameworks

The Institute agrees with the basic premise that the development of an effective risk appetite framework is an important component of sound risk management.[17] The Institute also concurs with the *Principles* that a 'top down' approach alone is not sufficient to be effective, but a RAF needs to be embraced and understood throughout a firm.[18] Hence, communication is a key enabler, both in the development of an effective RAF and in its effective operation.[19] This requires regular dialogue about risk appetite and evolving risk profiles among the board, senior management, the risk management function, and the businesses.

In the context of developing information technology and management information systems to be linked with RAFs footnote 4 of the RAF section of the *Principles* notes that "implementation of the *BCBS Principles for Effective Risk Data Aggregation and Risk Reporting* will facilitate firms' ability to identify, measure, aggregate and report on risks at the firm-wide, business line, legal entity and risk category levels." While, it is important that changes in RAFs be supported by relevant information technology (IT) and systems within institutions as the *Principles* suggests,[20] and in fact financial institutions continue to make significant investments in IT systems to support risk management generally[21] it would be helpful to clarify that full compliance with the effective data aggregation principles is not considered necessarily a pre-requisite for institutions' compliance with the risk-appetite framework.

In relation to communication of the RAF, *Principle* 1.1(a) goes further, stating that an effective RAF should "establish a process for communicating the RAF across and within the firm and, and to some extent, to external stakeholders". Owing to the fact that elements of a firm's RAF will include confidential business information, and that external communications are more generally governed, particularly in the United States and other jurisdictions, by securities law requirements, it would be useful to clarify that this *Principle* does not impose a requirement to disclose confidential information and should be viewed in the context of current applicable rules regarding disclosures. Furthermore, it would also be beneficial to clarify what "stakeholders" in this context means. Since there are different stakeholders such as counterparties, investors, vendors, and the like, disclosure responsibilities will vary in each case. Hence, a clearer view of this *Principle,* would help facilitate appropriate implementation.

Additionally, the RAF section of the *Principles* misses a few key elements. First, it seems to exclude models and systems that contribute to measuring and aggregating risk. This is important because, for instance, the lack of a robust risk weighting system in an

[17] IIF, *Implementing Robust Risk Appetite Frameworks to Strengthen Financial Institutions,* June 2011. Pg. 10
[18] Ibid. 11
[19] Ibid. 12
[20] *Principles,* Pg. 3
[21] IIF, *Remaking Financial Services: Risk Management Five Years After the Crisis,* July 2013. Pg. 66

institution's credit portfolios in one jurisdiction, could impact risk exposures measured under the established risk capacity and risk appetite. This is similar to our point above about defining risk capacity within the context of a firm's risk management capabilities and other considerations. Hence, it would be useful to mention the relevance of developing and employing the appropriate models to measure and estimate risk in setting the RAF.

Principle 1.1(b) refers to the "bottom up involvement of management at all levels" as well as top down board leadership in developing an effective RAF. This is a very important *Principle* as it captures the relevance of having an inclusive process. However, in some cases, it may be that the entirety of the information contained in the RAF, risk appetite statement and relevant reports is shared with a more limited group of senior managers in a firm (due to the sensitivity of that information when viewed altogether). That said, it is reasonable to expect a broad, more high level understanding of the RAF at all levels and that more junior managers have a robust understanding of what the RAF means for their businesses.

Secondly, *Principle* 1.1(f) discusses the adaptability of the RAF to changing business and market conditions – an idea which we strongly endorse. However, it further states that there may be instances where "an increase in the risk limit of a business line or legal entity may be counterbalanced by a reduction in the risk appetite allotment of another business line or legal entity…"[22] While we do not believe this is the intent, the current language may be interpreted to mean that the overall risk appetite has simply been divided up and allocated to individual legal entities or business lines without consideration of correlation effects. The current language also seems to presume that risk limits are fully utilized at all times, such that an increase in one risk area requires offset by reduction in another risk area. We believe it would be helpful for the *Principles* to emphasize that risk management (and risk appetite) is not a zero-sum exercise. There can be instances where risks in one legal entity or business line may be well understood to offset the risks in another. In such cases, increasing the risk limit of the legal entity/business line and at the same time reducing the risk limit in the other would rather reduce the offsetting effect, and hence would lead to an overall increase in group-wide risks. The overall view here is that risk limits are non-additive.

As an important, broader point, risk limits, which reflect risk appetite, are set inside risk capacity. If the risk capacity of the firm is increased in any way – for example, through a strengthening of the firm's risk management capabilities, perhaps following the implementation of a stronger risk technology system and risk data aggregation capability, or following the hiring of a new team of staff with extensive skills and experience in a particular business line, or following an increase in the level of the firm's capital - it may be fully appropriate to increase the limits in one or more particular business areas without changing the limits in any other area. Furthermore, the firm may simply decide to move its risk appetite closer to its risk capacity by increasing some limits for certain business areas, without decreasing others. This increase in limits – which reflects an increased risk appetite - can be appropriate.

[22] *Principles,* Pg. 4

Risk Appetite Statements

It is essential that the risk appetite be communicated in a statement that can be easily understood throughout the institution. The Institute notes the statement in *Principle* 2 that "setting the firm-wide risk appetite is the first step; the aggregate risk appetite has to be allocated to the firm's business lines, legal entities and down to all relevant levels, which need to align with the firm's strategic and business plans."[23] Similar to the point made in the above section about the non-additive nature of risk limits, due to the diverse and varying nature of business lines and legal entities, and the non-additive nature of their risks, it should not be assumed that risk appetite can be disaggregated and apportioned or allocated in all platforms of risk appetite statements. While the risk appetite of business lines should be aligned with the risk appetite statement of the firm, a clarification that recognizes this is not a precise or automatic process, but a highly qualitative/judgmental process, which involves bottom-up as well as top-down approaches will be very helpful. In addition, reinforcing our prior point, the quoted statement above also ignores the diversification that may exist across business lines. Moreover, a very top-down application of RAF could undercut business unit buy-in to the process and "ownership" of risk appetite.

Section 2.1(c) could be interpreted to require the establishment of risk appetite, risk capacity, and risk profile, for "each material risk" in a risk appetite statement. Risk appetite for instance, tends to be holistic and encompasses a variety of different operational elements that are relevant to constraining the maximum level of risk a firm can assume. Consequently, and due to the different nature of risks, it is not always clear how risk appetite, and some of the RAF elements can be broken down into various risk types, especially for non-quantifiable risks. We would therefore suggest that this be appropriately clarified.

Further, section 2.1(d) notes that quantitative measures that can be translated into risk limits applicable to business lines, legal entities and groups, which in turn can be aggregated and disaggregated, should be included in the risk appetite statement. It would be useful to recognize here the different kinds of risks that would not be easily quantified and aggregated, such as reputational risks. This would help broaden understanding of the application of the risk appetite statement.

In the subsequent bullet, 2.1(e), the *Principles* recognizes that risk appetite statements should include qualitative statements for risks that are not easy to measure. It further adds that "boundaries or indicators" need to be established to enable monitoring of these risks. The recognition of the relevance of qualitative statements as an important aspect of a risk appetite statement is very welcome. The Institute would further highlight that boundaries of acceptable risk-taking are often qualitative in nature, and in a number of cases, quantitative boundaries would not be possible. A reflection of this emphasis in the *Principles* would help provide a more complete understanding of the development of risk appetite statements.

Section 2.1(g) requires that elements of a risk appetite statement are "…forward looking and subject to scenario and stress testing…" Indeed, it is useful to apply some stress tests in developing risk appetite statements to understand what might cause firms to exceed their risk appetite. However, it is unclear whether this *Principle* suggests that firms would be

[23] ***Principles,*** Pg. 4

required to develop risk appetite statements towards the most conservative expectations of stress testing. We do not believe that this is the intent or should be the case, thus this should be clarified. Otherwise, it will lead to concentration and contagion risk, with all firms pursuing what is viewed as the safest business strategy, rather than the development of a healthy diversity of business models and strategies.

Risk Limits

The opening paragraph of the risk limits section, notes that "having risk limits that are measureable can prevent a firm from unknowingly breaching risk limits as market conditions change and be an effective brake against excessive risk-taking."[24] The general point in the paragraph about the effectiveness of risk limits as a brake against excessive risk-taking is clear. However, with regard to the quoted statement, it seems unclear how risk limits that have not yet been set would unknowingly be breached. This seems to suggest there might be risk limits that are unmeasured or unstated. Further clarification here would foster a better understanding.

Section 3.1(a) indicates that a risk limit should be set at a level to constrain risk-taking within risk appetite based on an estimate of the impact on a variety of stakeholders including customers, shareholders, capital etc. in case the limit is breached. This principle seems to suggest a requirement for an impact analysis of the breach of risk limits on a number of interests and stakeholders, which would be unusual since business lines tend to be diversified and a risk limit may involve qualitative aspects and would overall not lend itself to a rigorous analysis. This may be a misinterpretation of the principle and further elaboration would be useful in clarifying this section.

Section 3.1(c) says risk limits should "include material risk concentrations at the firm-wide, business line and legal entity levels (e.g., counterparty, industry, country/region, collateral type, product)." The Institute would note that this is a useful principle, but would emphasize that the concept of materiality and proportionality mentioned above, is applied when risk limits are contemplated for exposures at the business line or legal entity level.

One of the challenges to implementing effective RAFs is the lack of uniform processes to translate high-level risk appetite indicators into more specific measures - including risk limits.[25] It is unarguably important to have a clear and structured set of limits; however, it may be helpful to make a distinction between limits that can be easily controlled, such as lending volumes, and metrics like average loan-to-value (LTV), which are more difficult to control ex ante.

Furthermore, in the IIF report *Implementing Robust Risk Appetite Frameworks to Strengthen Financial Institutions* it was noted that there has been a recent trend whereby organizations refine and reduce the number of quantitative and qualitative metrics used for risk appetite purposes.[26] Some firms have found that too many metrics can make it difficult

---

[24] *Principles,* Pg. 5
[25] IIF, *Implementing Robust Risk Appetite Frameworks to Strengthen Financial Institutions,* June 2011. Pg. 22
[26] Ibid. Pg. 23

to hold individual businesses accountable. Getting the number of metrics right can be a challenging balancing exercise. Including high-level metrics in risk appetite statements enables staff to understand what risk appetite means for them.

In the context of applying risk limits to business lines or legal entities, as principle 3.1(c) requires, it will be useful here, as discussed above that a materiality test and a measure of proportionality is considered.

Finally, section 3.1(d) cautions that risk limits should "not be strictly based on comparison to peers, default to regulatory limits, be overly complicated, ambiguous, or subjective…" It seems two distinct points are being made in this context and may require further clarification so the *Principle* can be correctly interpreted and applied. The *Principle* could be interpreted as saying (a) risk limits should not be strictly based on comparison to peers or default to regulatory limits, but should reflect the institution's risk appetite, and (b) risk limits should not be overly complicated, ambiguous, or subjective. Both points could be separate principles, and would be in line with the Institute's thinking as indicated above, with regards to having the right balance of metrics that can be comprehended and applied firm-wide.

Roles and Responsibilities

- *Board of directors:*

We recognize that the *Principles* document "does not advocate a specific board structure"[27] owing to the jurisdictional and organizational differences among institutions. This is a welcome approach and would provide opportunity for institutions to tailor the *Principles* to their organizational frameworks and legal environments within which they operate. However, the Principles should avoid creating specific roles and obligations for specific structures, which might not be applicable across all jurisdictions. We note for example that in the case of institutions that have Supervisory Boards (for general oversight) and Executive Boards (for actual management), a few of the responsibilities identified, say in 4.1(a), 4.1(b), and 4.1(d), may only apply to their Supervisory Boards, while the rest will fall under the responsibility of the Executive Board. It would be useful to clarify in the *Roles and Responsibilities* section these differences to avoid the Supervisory Board (in a two-tier board system) being responsible for roles they may not be equipped for.

We strongly agree that the board of directors plays an important role in the oversight of the development of the RAF and its implementation. However, the Principles should recognize the distinct roles and responsibilities of a company's board of directors and senior management. In certain areas, the Principles seem to require senior management-type execution responsibilities from the boards, which would not be suited to the effective performance of boards' supervisory and monitoring role. The board has the final responsibility for monitoring risk matters, and as a result, their engagement is essential to achieving the right balance between rigidity and flexibility in the RAF.[28] However, beyond

[27] *Principles,* Pg. 6 (footnote 6)
[28] IIF, *Implementing Robust Risk Appetite Frameworks to Strengthen Financial Institutions,* June 2011. Pg. 13

that, the procedural terms or mechanisms that a board may use to carry out its function should be based on the organizational structure and the board's internal management approaches.

Specifically, in section 4.1(e), the Board is required to "regularly review and monitor actual versus approved risk limits…" A common practice, and perhaps what might be more useful to the Board from a risk governance point of view, would be to review reports from management on actual or forecasted results that have exceeded or are projected to exceed risk appetite tolerances. However, the specifics of the information and documentation that the board should review must be based on the discretion of the institution.

Principle 4.1(f) requires the board of directors to "discuss and determine actions to be taken, if any, regarding 'breaches' in risk limits." As noted above, the board has final responsibility for monitoring risk matters and for approving general risk governance policies. However, the board does not actively manage a firm's day-to-day risk issues; the board meets periodically and reviews and monitors the performance of senior management in managing risk. Subject to board oversight (and, ultimately, regulatory review), firms should grant senior management flexibility when responding to breaches in risk limits, recognizing that it is difficult to know in advance the causes of a specific breach or which remedial actions will actually reduce risk.

- *Senior management:*

In relation to senior management, the roles outlined in the *Principles* are important, and it is essential for senior management to understand what their roles are in the RAF development, implementation, and monitoring processes, as they continuously collaborate to maintain a robust RAF. It is also important that they have mechanisms in place to help them to move rapidly to address any risks that may emerge. However, the *Principles* should identify key risk appetite and risk management functions to be performed within a firm by senior management rather than prescribe which officers must perform specific functions. Banking organizations have adopted diverse corporate governance forms in response to varying business models, regulatory requirements, and geographic scope of operation. The *Principles* should avoid being overly prescriptive and should instead provide firms with the flexibility to implement risk appetite frameworks that are tailored to, and appropriate for, their specific organizations. Where there appears to be specific deviations from the *Principles,* there should be opportunity for individual institutions to explain their approaches and how they may be broadly aligned with the objectives of the *Principles* as finalized.

Furthermore, the Institute would emphasize that "neither the risk function nor the CRO 'owns' risk, nor can either be involved in policing every risk decision made throughout the organization."[29] Therefore, the fundamental ownership of risk (meaning taking responsibility for monitoring risks, identifying new or emerging risks, containing risks within the RAF, and balancing risk and opportunity within the RAF) resides in each specific business based on the organization's structure and governance framework, not just in the

[29] IIF, *Governance for Strengthened Risk Management,* October 2012. Pg. 37

risk function. However, the board, in collaboration with senior management, plays an important oversight role, even though that role may take different forms in different organizations (for example, some organizations may have risk committees, which have membership from the risk and business areas, which take more direct leadership in overseeing risk). This point is central to the development of the RAF, risk appetite statement, risk limits, and other components of the RAF. It is a key aspect that fosters the iterative and evolutionary process, because as business units apply the RAF, they will determine what changes are necessary throughout the process and would take responsibility for conveying information upstream.

It seems clear that the *Principles* are trying to promote cooperation among senior executives, which is a very necessary principle. However, in many cases it seems as though the roles of the Chief Executive Officer (CEO), Chief Risk Officer (CRO), and Chief Financial Officer (CFO), are addressing the same subject matter. While there might be different degrees of emphasis in terms of the roles that senior executives might be playing, becoming overly prescriptive in attempting to define individual roles and responsibilities can have the effect of confusing, and creating distinctions without a meaningful difference. A universal model could unnecessarily restrict an organization's ability to delegate appropriately within a governance framework that meets the unique requirements of its organizational structure.

- *Internal audit:*

An issue of concern is the proposed role of *internal audit* (or other independent assessor) in a firm's RAF development and evaluation process. The *Principles* mandate a new role for internal audit to assess the RAF on a firm-wide basis as well as on an individual business line and legal entity basis, and further include other roles that may be excessive. Essentially, some assessment of the overall effectiveness of the core areas of the RAF, taking a high-level and non-granular approach, is appropriate and useful. While it is appropriate to have independent checks on the RAF process, internal audit may not always be the appropriate function to take up such tasks. Furthermore, the level of internal audit review will be limited by the institution's capability and bandwidth of resources. As a result, the *Principles* should remain agnostic on that organizational point but focus on what should be the purposes and expected outcomes of an independent review process.

The Basel Committee on Banking Supervision's report of June 2012 on *The Internal Audit Function in Banks* requires the internal audit to be responsible for the "evaluation of risk appetite, escalation and reporting of issues and decisions taken by the risk management function."[30] This responsibility with respect to risk appetite is a fairly more modest role than the role described in the *Principles,* which requires annual assessments and validations of the design and effectiveness of the RAF, routine firm-wide and individual business line and legal entity level RAF assessments, evaluation of the need for supplemental assessments, and the

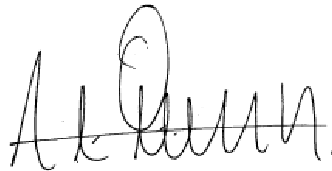
[30] The Basel Committee on Banking Supervision, *the Internal Audit Function in Banks,* June 2012. Pg. 8

like.[31] This tends to be outside of the generally understood scope and role of the internal audit function.

3. Conclusion

As indicated at the outset of this letter, the Institute welcomes the development of the FSB *Principles*, and believes that they will go a long way to enhance RAFs that are already being established by institutions across many jurisdictions. The issues raised are primarily meant to provide some key areas of emphasis, where uncertainty could lead to implementation divergence and challenges. The Institute is ready to provide further input through this consultation process.

Sincerely,



[31] *Principles,* Pg. 10 (4.6 (a) to (g)).