Richard F. Chambers
Certified Internal Auditor
Certified Government Auditing Professional
Certification in Control Self-Assessment
Certification in Risk Management Assurance
*President and Chief Executive Officer*

T: +1-407-937-1200
E-mail: richard.f.chambers@theiia.org

January 31, 2014

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

Dear Mr. Andresen,

RE: FSB Consultative Document - Guidance on Supervisory Interaction with Financial Institutions on Risk Culture

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) Guidance on Supervisory Interaction with Financial Institutions on Risk Culture Consultative Document. As the global standards-setting body for the professional practice of internal auditing, we appreciate the opportunity to provide comment on this guidance and fully concur with the concept of increasing the intensity and effectiveness of supervision for the promotion of a sound risk culture within financial institutions.

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 Consultative Document are below. Additional, more detailed observations and comments are provided in Attachment A.

Overall the Consultative Document 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) Financial institutions are profitable and provide shareholder value over the long-term by prudently managing risk taking activities. Although the Consultative Document refers to prudent "risk taking" in the *Compensation* and *Incentives* sections, much of the Consultative Document is written with a slant toward risk avoidance. Generally, risk culture should be about creating an environment where undertaking risk on behalf of the institution is done consistent with the management of risk within tolerance levels approved by the board and senior management.

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

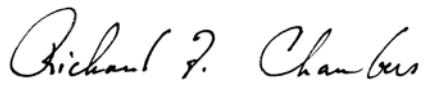
2) Consider including or referencing additional guidance that would be useful to both the institution and the supervisor, when applying this particular guidance. For example,

   Within section three on "General Supervisory Guidance", the Consultative Document states, "In particular, supervisors should assess how the board and senior management systematically assess the risk culture of the institution, and document what they are finding and how any deficiencies in risk culture are addressed. The institution's willingness to sufficiently document the elements supporting its risk culture should form part of the supervisor's overall assessment." We suggest that additional guidance may be necessary to supplement a supervisor's ability to successfully assess an institution's risk culture, document findings, review remediation plans and determine an institution's willingness to document elements of its own risk culture.

Please do not hesitate to contact Glenn Darinzo, IIA's Director of Standards and Guidance, 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. Mr. Darinzo can be reached via email: glenn.darinzo@theiia.org or phone 1-407-937-1164.

Again we applaud the efforts of the FSB to promulgate guidance for the promotion of a sound risk culture within financial institutions. I look forward to an opportunity to meet you in the future to continue our discussions and further build awareness of the critical role internal auditing can and does play in ensuring good governance, risk management and internal controls thereby enhancing financial stability within financial institutions and other organizations.

Best Regards,



Richard F. Chambers, CIA, CGAP, CCSA, CRMA
President and Chief Executive Officer

# Attachment A
# Specific Recommendations/Comments

| Section | Recommendations/Comments |
|---|---|
| **General Comments** | |
| General | Be consistent by replacing firm or organization with "institution." |
| General | The last section on Talent Development and Succession Planning refers to "training programs that are available for all staff to develop risk management competencies." However, training on risk identification and risk assessment has a significant impact on a financial institution's risk culture. Suggest providing more detailed descriptions of training such as, risk assessment, risk culture, risk appetite, tolerance levels, risk statements, and overall risk management. Also suggest addressing different types and the frequency of training required. |
| General | The Consultative Document should include some additional tools to assist the supervisors in effectively assessing the risk culture of financial institutions. Specifically, within section three on "General Supervisory Guidance", the guidance states that "supervisors are in a unique position to assess risk culture" and that "assessing risk culture is embedded in every supervisory activity." However, the guidance does not provide details or tools to assist the supervisor in how to evaluate a financial institution's risk culture. Additionally, the guidance does not include the polling of external stakeholders in their assessment of the financial institution's risk culture. In both instances, it would be helpful in assisting supervisors to include tools such as interviews at all levels within the institution, internal and external surveys, and risk assessment workshops (or focus groups) that would be beneficial when evaluating an institution's risk culture. |
| **2. Indicators of a sound risk culture** | |
| First bullet | "Tone from the top: The board of directors and senior management are the starting point for setting the financial institution's core values and risk culture, and their behaviour must reflect the values being espoused. This would include ensuring adequacy of investments in key governance and risk management resources to include people, processes and systems. As such, the leadership of the institution should systematically develop, monitor, and assess the culture of the financial institution." |
| **3. General supervisory guidance** | |
| 3rd paragraph | "In particular, behaviours that underpin supervisory findings should be highlighted to the board, which has ultimate responsibility for outlining, directing and overseeing the financial institution's risk culture. The supervisor raising, and the financial institution acting early to address, the root causes of ~~the~~ actual or suspected behavioural weakness will aid in preventing (or mitigating the impact of) particular undesired cultural norms ~~from taking root and growing~~deviating from the board's expectations." |
| **3.1 Tone from the top** | |
| 1st paragraph | "Non-executive directors can play an important role in bringing experience from other ~~industries~~financial institutions or companies in other regulated industries where behaviours and practices generally necessitate a sound risk culture ~~(e.g., healthcare, nuclear energy)~~ and often are well placed to bring a fresh perspective and sage advice about issues such as behaviour in relation to overall culture."<br><br>and<br><br>"The appropriate tone and standard of behaviour 'from~~at~~ the top' is a necessary condition for promoting sound risk management. However, it is far from sufficient. For lasting change, the tone and behaviour 'in the middle' (e.g., middle management actions that reinforce the 'tone from the top'), and indeed throughout the institution, is also important." |
| **Indicators of tone from the top** | |

| Section | Recommendations/Comments |
|---|---|
| 3.1.1 | "The board and senior management are committed to establishing, monitoring, and adhering to an effective risk appetite ~~statement~~framework, supported by appropriate risk appetite statement(s) that underpin~~s~~ the financial institution's risk management strategy and are integrated with the overall business strategy." |
| 3.1.3 | "The board and senior management promote through behaviours, actions and words a risk culture that expects integrity and a sound approach to risk management." |
| 3.1.4 | "The board and senior management promote ~~an open exchange of views, challenge and debate, including~~ healthy skepticism that encourages and supports openness to challenge those in authority by providing alternative points of view that may result in a better decision, ensuring that all directors have the tools, resources and information to carry out their roles effectively, particularly in exercising their challenge function." |
| 3.1.5 | "The board and senior management have mechanisms in place~~, such as talent development and succession planning,~~ which help to lessen the influence of dominant personalities and behaviours. For example, a robust confidential 360 degree review process can help identify such personalities and result in appropriate coaching." (Rationale for proposed changes: While talent development and succession planning are important factors, there are many other important factors.) |
| 3.1.6 | "…throughout the institution as a whole is ~~the same as~~consistent with the 'tone ~~at~~from the top'." |
| 3.1.7 | "The board and senior management have mechanisms in place to assess whether the risk appetite framework, the risk appetite statement(s), risk management strategy and overall business strategy." (Rationale for proposed changes: It all starts with the RAF, and there could be more than one risk appetite statement.) |
| 3.1.9 | "The board and senior management demonstrate a clear understanding of the quality and consistency of risk management decision-making throughout the business, including how risk is ~~decision-making is~~ understood and how that understanding should influence decisions consistent with the financial institution's risk appetite and the business strategy." |
| 3.1.10 | "The board and senior management have clear views on the business lines considered to pose the greatest challenges to risk management ~~such as unusually profitable parts of the business,~~ and these are subject to constructive and credible challenge about the risk-return balance." |
| 3.1.11 | "The board and senior management systematically monitor how quickly issues raised by ~~the board~~themselves, supervisors, external audit, internal audit, ~~and other~~as well as by any second line of defense control functions are addressed by management." |
| 3.1.12 | "…to the ~~firm~~institution, are reviewed at ~~all~~the appropriate levels of the ~~organization~~institution and are seen as an opportunity to strengthen the financial institution's risk culture ~~and make it more robust~~." (Rationale for proposed changes: "strengthen" and "robust" seemed synonymous.) |
| 3.1.13 | "Assessment and communication of lessons learned from past ~~errors~~events is seen as an opportunity to enhance and/or strengthen the institution's risk culture~~, and to enact real changes for the future~~." (Rationale for proposed changes: Events is a broader term and lessons can be learned from things other than "errors," and "real changes for the future" seemed unnecessary to make this point.) |
| **3.2 Accountability** | |
| 1st paragraph | "In particular, business lines, the risk management function, ~~and~~ internal audit and all applicable second line of defense functions (e.g., compliance, security, etc.) should have clearly delineated responsibilities in regard to assessment, monitoring, identification, management and mitigation of, as well as reporting on, risk. Accountability speaks to the prompt identification, management, and escalation of emerging and unexpected risk issues, and having a clear understanding of the consequences for not doing so, while retaining ~~ownership~~day-to-day operating management of risk with the units originating them." |
| **Indicators of accountability** | |
| 3.2.2 | "Mechanisms are in place for the ~~lines of business to share~~ sharing of information on emerging ~~and unexpected risks, including horizontally to other business lines and units that might be impacted~~, as well as low probability, high impact risks, both horizontally across business lines and vertically up the institution." (Rationale for proposed changes: Information sharing is more than just across business lines. Also, the term "unexpected risks" seems incorrect, since it is not a risk if you don't expect it even remotely. So, low probability, high impact risks may get at the point intended more generally (e.g., "black swans".) |

| Section | Recommendations/Comments |
|---|---|
| 3.2.3 | "Employees are held accountable for their actions and are aware of the consequences for not adhering to the desired risk management behaviours~~,~~ regardless of whether their actions resulted in financial gain or loss to the financial institution.~~, and are aware of the consequences for not adhering to the desired risk management behaviour~~." |
| 3.2.6 | "Mechanisms are established for employees to ~~raise~~elevate and report concerns when they feel discomfort about products or practices, even where they are not making a specific allegation of wrongdoing~~, and for acting on those concerns~~." (Rationale for proposed changes: To clarify what "acting on concerns" means, by using "elevate and report" language.) |
| 3.2.8 | "Consequences are clearly established, articulated and applied for ~~business lines or individuals~~ anyone engaged in, or supporting, risk-taking that is excessive relative to…" |
| 3.2.9 | "Breaches in internal policies, procedures and risk limits, as well as non-adherence to internal codes of conducts~~s~~, are understood to have a potential impact on an individual's compensation and responsibilities, ~~or~~can affect career progression and, depending on severity, may result in~~ including~~ termination." |
| **Stature of risk management** | |
| 3.3.3 | "The chief risk officer~~, and~~ risk management function and internal audit share the same stature as the lines of business, actively participating in senior management committees and proactively being involved in all ~~the~~ relevant risk decisions." |
| 3.3.4 | "The chief risk officer, the ~~and~~ risk management function and internal audit have appropriate direct access to the board and senior management and effectively utilize it." |
| 3.3.5 | "Compliance, legal, internal audit and other second line of defense control functions…" |
| **Indicators of incentives** | |
| 3.4.2 | "…promote the financial institution's desired core values, compliance with policies and procedures~~, internal audit results,~~ and address internal control deficiencies and supervisory findings timely." (Rationale for proposed changes: Internal audit results are secondary to the seriousness and timeliness with which management addresses control deficiencies, regardless of who identifies such deficiencies (e.g., internal audit, external audit, supervisory agencies, etc.) |
| 3.4.5 | "Succession planning processes for key management positions include risk management experience, to include individuals with responsibilities consistent with that of being ~~and not only revenue-based accomplishments; for instance,~~ the chief risk officer, chief compliance officer and chief internal audit officer ~~can be considered as a~~ as potential candidates for ~~chief executive officer~~other C-level executive positions, including the chief executive officer." (Rationale for proposed changes: It is implied that "not only revenue-based accomplishments" are part of this by the way it is worded.) |