Richard F. Chambers
Certified Internal Auditor
Qualification in Internal Audit Leadership
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

09 January 2015

Basel Committee on Banking Supervision

RE: Consultative document: *Corporate governance principles for banks*

On behalf of the more than 180,000 global members of The Institute of Internal Auditors (IIA), I am pleased to provide our general observations and specific comments on the Basel Committee on Banking Supervision's consultative document, *Corporate governance principles for banks.* Our observations and comments were developed by a team of leaders in the internal audit profession, representing The IIA's global reach and financial services sector experience.

The IIA welcomes revisions to *Corporate governance principles for banks* that include strengthened guidance regarding the role of the board, the key role and responsibilities of risk management as part of the second line of defense, and the general references to the Three Lines of Defense model. In addition, we fully support the requirement under Principle 10 for "internal auditors to adhere to national and international professional standards" and appreciate the specific reference to The IIA's globally recognized Standards. This requirement is consistent with Basel's 2012 guidance, *The internal audit function in banks.*

The IIA believes that *Corporate governance principles for banks* could be further strengthened by providing additional guidance on compliance, and by clarifying and distinguishing internal audit as the third line of defense assurance function, not as a control function. Detailed comments in support of these and other observations are provided in Attachment A.

Thank you for the opportunity to provide our observations and comments on this consultative document. If you have any questions about this response and/or would like to schedule a time for us to meet in person or via conference call, please contact Stacy Mantzaris, The IIA's Managing Director of Global Advocacy, at stacy.mantzaris@theiia.org or +1-407-937-1290.

Best regards,

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

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

Legend
~~Strikethrough.~~ Text deleted from consultative document.
Underline: Text added to the consultative document.
Underline and bold: Text added to the consultative document with emphasis.

Attachment A
Specific Comments and Observations

Glossary

The inclusion of a glossary at the beginning of the document helps to ensure that diverse global readers will have a common understanding of terms used throughout the document. The IIA believes that it would be valuable to expand and modify the glossary to include additional key terms and provide clarification between similar terms. Our suggestions include:

1. *Control functions*: Consistent with the Three Lines of Defence[1] model, internal audit is widely recognized as an internal assurance function, not a control function. We believe that the wording of this definition causes confusion. From our perspective, functions that own, implement, manage, and oversee risks are control functions. Functions that provide independent assurance on the effectiveness of governance, risk management, and controls are assurance functions. Consider changing the definition of "control function" and adding a definition for "assurance function," accordingly.
2. The exposure draft uses the terms "corporate culture" and "risk culture," but provides a definition only for "risk culture." Consider providing a definition for "corporate culture," as well. Such definitions should clearly differentiate between corporate culture and risk culture. (Arguably, risk culture is a subset of an organisation's overall [corporate] culture.) As an example, in describing culture and ethical behaviour, the International Corporate Governance Network (ICGN) states that "Companies should engender a corporate culture which ensures that employees understand their responsibility for appropriate behaviour. The board should seek actively to cultivate and sustain an ethical corporate culture in the company. The company should take active measures to ensure that its ethical standards are adhered to in all aspects of its business."[2]
3. *Internal control system:* The wording of this definition may cause role confusion between the second and third lines of defence. Suggested revision:
   Internal control system: A set of rules and controls governing the bank's organisational and operational structure including reporting processes ~~and functions for risk management, compliance and internal audit.~~ and control functions, such as compliance, risk management, security, and quality. Internal audit is responsible for independently assessing and reporting on the internal control system.
4. *Risk limits*: Consider adding to the existing definition:
   Other terms for risk limits include risk-bearing capacity[3,4] and risk tolerance.[5]
5. Consider adding definitions for the terms "accountability" and "responsibility." The distinction between these two concepts is important. In our view, a function has "accountability" if it has to answer for something, and a function has "responsibility" if it has to "do" something. For example, the board of directors is ultimately "accountable" for corporate governance. The board has to answer to regulators, investors, employees, other stakeholders, and society in general regarding

[1] The IIA's Position Paper, The Three Lines of Defense in Effective Risk Management and Control, 2013.
[2] ICGN Global Corporate Governance Principles: Revised 2009, International Corporate Governance Network, p.15.
[3] The King Code of Governance for South Africa 2009 (King III), Institute of Directors in Southern Africa, p. 58.
[4] ICGN Global Corporate Governance Principles: Revised 2009, International Corporate Governance Network, p. 17.
[5] Enterprise Risk Management – Understanding and Communicating Risk Appetite 2012, The Committee of Sponsoring Organizations of the Treadway Commission (COSO), p.4.

Legend
~~Strikethrough.~~ Text deleted from consultative document.
Underline: Text added to the consultative document.
Underline and bold: Text added to the consultative document with emphasis.

governance of the organisation. On the other hand, the board is "responsible" for governance oversight. Oversight is what the board "does" when it performs activities such as reviewing external and internal audit reports.

Introduction

Paragraph 2

Consider the following revision:

Corporate governance ~~determines~~ sets the parameters for the allocation of authority and responsibilities by which the business and affairs of a bank are carried out by its board and senior management, including how they:

- are selected/elected
- set the bank's strategy and objectives;
- select and oversee personnel;
- operate the bank's business on a day-to-day basis;
- protect the interests of depositors, meet shareholder obligations, and take into account the interests of other recognised stakeholders;
- align corporate culture, corporate activities and behaviour with the expectation that the bank will operate in a safe and sound manner, with integrity and in compliance with applicable laws and regulations, and codes of ethics;
- act and communicate in a transparent manner; and
- establish control functions.

Corporate governance does not determine these things, people do. The suggested edits will make that distinction and also strengthen alignment with paragraphs 23 and 27, and Principles 2 and 12.

Paragraph 9

In the next to last sentence, consider changing "CRO and internal audit" to "risk management, compliance, and internal audit."

Paragraph 11

Edit the fifth sentence as follows:

"The compliance function is also ~~deemed~~ part of the second line of defence." Elimination of the word "deemed" definitively makes compliance part of the second line of defence and eliminates misinterpretation.

Edit the sixth sentence as follows:

"The internal audit function is charged with the third line of defence, conducting risk-based and general audits and reviews to, among its responsibilities, provide assurance to the board that the overall corporate governance framework, including the risk governance framework, is effective, ~~and~~ that appropriate policies and processes are in place and that they are consistently applied."

Principle 1: Board's overall responsibilities

The emphasis on the board establishing a sound corporate culture in Principle 1 is particularly welcome. Its importance has been widely recognized in analyzing the underlying causal factors of the most recent financial crisis. The concept of corporate culture might be expanded to include various aspects such as the

risk and control culture of the organisation; the customer-facing culture with regard to the organisation acting with integrity toward its dealings with customers and markets; and the design and operating effectiveness of policies and processes to ensure that they in line with the objectives, risk appetite, and values of the organisation. See our suggestions at paragraph 28.

Paragraph 20

The IIA's perspective is that **management has responsibility** (not the Board, as stated in this paragraph) for the bank's business strategy and financial soundness, key personnel decisions, internal organisation and governance structure and practices, and risk management and compliance obligations. The **board**, however, **has ultimate accountability** for ensuring that management fulfills these responsibilities. See Glossary comment #5.

We recommend a clarifying addition that indicates who the board is accountable to:

> The board is accountable to the bank's shareholders, stakeholders, and supervisors for effective governance oversight.

Such statements of accountability are made regarding senior management and the internal audit function in Paragraph 86 and Principle 10, respectively, but not for the board.

Paragraph 21

At footnote 10, we recommend changing "responsibility" to "accountability," consistent with our other commentary.

Paragraph 23

The word "established" is used in the first two bullet points. Consistent with our comments regarding differentiating management and board accountability versus responsibility, we recommend the following changes:

- ~~establish~~ approve and monitor the bank's business objectives and strategy;
- ~~establish~~ influence and oversee the bank's corporate culture and values

Paragraph 26

After paragraph 26, consider adding a paragraph setting expectations for any key second line of defence leaders (e.g., chief risk officer, chief compliance officer, chief ethics officer) to report, at least annually, directly to the board, without filter from management.

Paragraph 28

Consider adding the following bullet:

- seeking objective, independent assurance that the "tone at the top" and associated desired culture and values are properly reflected in actions and decisions throughout the organisation. (This can be part of internal audit's third line of defence activities.)

Paragraph 30

Second bullet, consider revising as follows:

- The board should have oversight of the whistleblower policy and mechanisms, seeking independent assurance that they are working effectively, and ensuring that senior management addresses legitimate issues that are raised. ~~There should be direct or indirect communications to the board (eg through an independent audit or compliance process or through an ombudsman independent of the internal "chain of command".~~

Legend
~~Strikethrough.~~ Text deleted from consultative document.
Underline: Text added to the consultative document.
Underline and bold: Text added to the consultative document with emphasis.

Third bullet: Consistent with our earlier comments regarding accountability versus responsibility, the board should not determine how or by whom legitimate concerns shall be investigated. Consider replacing the third bullet point with the following:

- The board should oversee or supervise management's efforts to develop:
  a. a reporting mechanism for the receipt and retention of complaints, and
  b. comprehensive investigation procedures, including types of investigations, roles and responsibilities for conducting investigations, escalation procedures, procedures for notifying regulatory authorities when applicable, and consistent enforcement across all levels of the organisation. Internal audit should be informed of investigation results.

Paragraph 41

It should be clarified that the third line of defence reviews the work of the second line of defence. Distinguishing features of internal audit are its independence from executive management and its ability to provide objective assurance to the board. Consider revising Paragraph 41 as follows:

> The third line of defence consists of an independent and effective internal audit function. Among other things, it provides independent review and objective assurance on the quality and effectiveness of the bank's internal control system, the first and second line of defence, and the risk governance framework including links to organisational culture, as well as strategic and business planning, compensation and decision-making processes. Internal auditors must be competent and appropriately trained and not involved in developing, implementing or operating the risk management function or other second line of defence functions (see Principle 9).

Paragraph 42

For clarification, consider the following revision:

> The board should ensure that the risk management, compliance and internal audit functions are properly positioned, staffed and resourced and carry out their responsibilities independently, objectively, and effectively. In the board's oversight of the risk governance framework, the board should regularly review policies and controls with senior management and with the heads of the risk management, compliance and internal audit functions to identify and address significant risks and issues, as well as determine areas that need improvement.

Paragraph 43

Consistent with our earlier comments regarding accountability versus responsibility, and clarifying that internal audit is an assurance and advisory function, consider the following revisions:

> The board should select the CEO and ~~may~~ oversee and approve the selection of other key members of senior management, as well as the heads of internal audit and any key second line of defence functions. ~~key members of senior management, as well as the heads of the control functions.~~

Principle 2: Board qualifications and composition

There should be term limits for directors, particularly independent directors. Consider adding a paragraph that addresses term limits.

Paragraph 47

Consider the following revision:

> Board members should have a range of knowledge and experience in relevant areas and have varied backgrounds to promote diversity of views. Relevant areas of competence include, but are not limited to, financial and capital markets, financial analysis, financial stability, financial

reporting, accounting, IT, strategic planning, risk management, compensation, regulation, corporate governance and management skills.

Paragraph 49

Consider the following revision:

The selection process should include reviewing whether board candidates: (i) possess the knowledge, skills, experience and independence of mind given their responsibilities on the board and in the light of the bank's business and risk profile; (ii) have a demonstrated record of unparalleled integrity and good repute; and (iii) have sufficient time to fully carry out their responsibilities.

Principle 3: Board's own structure and practices

Paragraph 67

For clarification, consider the following revision:

The audit committee:

- is required for systemically important banks. For banks of large size, risk profile or complexity it is strongly advised. For other banks it remains strongly recommended.
- is required to be distinct from other committees.
- should have a chair who is independent and is not the chair of the board or any other committee.
- should be made up entirely of independent or non-executive board members.
- should include members who have experience in internal and external audit practices and financial literacy at banks.

Paragraph 68

The IIA believes that this section could be strengthened by the following revisions:

The audit committee is responsible, among other things, for:

- the financial reporting process;
- providing oversight of and interacting with the bank's ~~internal and~~ external auditors;
- providing oversight of the bank's internal audit function, ensuring that it is independent of senior management and has the appropriate standing, access, and authority;
- approving the internal audit plan;
- approving, or recommending to the board or shareholders for their approval, the appointment, compensation and dismissal of external auditors;
- approving, or recommending to the board or shareholders for their approval, the appointment, compensation and dismissal of the chief audit executive;
- reviewing and approving the audit scope and frequency;
- receiving key internal audit reports and ensuring that senior management is taking necessary corrective actions in a timely manner to address control weaknesses, non-compliance with policies, laws and regulations and other problems identified by internal auditors and ~~other~~ control functions;
- overseeing the establishment of accounting policies and practices by the bank; and

- reviewing the third-party opinions on the design and effectiveness of the overall risk governance framework and internal control system.

Paragraph 70

Add the following bullet:

- should have direct interaction with the chief audit executive, and ensure there is positive and constructive collaboration between the chief risk officer and the chief audit executive.

Paragraph 75

In the second sentence, clarify whether the word "culture" refers to risk culture, organisational culture, or both.

Principle 4: Senior management

Paragraph 90

Consider the following revision:

> Senior management contributes substantially to a bank's sound corporate governance through personal conduct (e.g. by helping to ~~set~~ establish the "tone at the top" along with the board). Members of senior management should provide adequate oversight of those they manage, and ensure that the bank's activities are consistent with the business strategy, risk appetite and the policies approved by the board.

Paragraph 92

Internal audit should not be included as a second line of defence implemented by senior management. Consider the following revision:

> Senior management should implement, consistent with the direction given by the board, risk management systems, processes and controls for managing the risks – both financial and non-financial – to which the bank is exposed and for complying with laws, regulations and internal policies.

- This includes comprehensive and independent risk management, compliance and ~~audit~~ other second line of defence functions, as well as an effective overall system of internal controls.
- Senior management should recognise and respect the independent duties of the risk management, compliance and internal audit functions and should not interfere in their exercise of such duties.

Principle 5: Governance of group structures

Paragraph 95

Consider adding the following bullet:

- maintain an effective internal audit function that ensures audits are being performed within or for all subsidiaries and parts of the group and the group itself;

Paragraph 97

The IIA believes that subsidiary corporate governance responsibilities are not fully independent from the parent company's corporate governance responsibilities. Consider the following edit:

> In the case of a significant regulated subsidiary (due to its risk profile or systemic importance or due to its size relative to the parent company), the board of the significant subsidiary should take

Legend
~~Strikethrough.~~ Text deleted from consultative document.
Underline: Text added to the consultative document.
Underline and bold: Text added to the consultative document with emphasis.

such further steps as are necessary to help the subsidiary meet its ~~independent~~ own corporate governance responsibilities and the legal and regulatory requirements that apply to it.

Principle 6: Risk management

Paragraph 105

Consider the following revision:

The risk management function should have a sufficient number of personnel who possess the requisite experience and qualifications, including market and product knowledge as well as command of risk disciplines. Staff should have the ability and willingness to effectively challenge business ~~lines~~ operations regarding all aspects of risk arising from the bank's activities.

Paragraph 108

"Dual hatting" as a corporate governance weakness is applicable to all lines of defence, not just the CRO. Consider clarifying this language throughout the document. Also, consider including the ability for a comply-or-explain option to be utilized in situations where "dual hatting" exists.

Principle 7: Risk identification, monitoring and controlling

Paragraph 111

Consider the following revision:

Risk identification should encompass all material risks to the bank, on- and off-balance sheet and on a group-wide, portfolio-wise and business-line level. In order to perform effective risk assessments, the board and senior management, including the CRO, should, regularly and on an ad hoc basis, evaluate the risks faced by the bank and its overall risk profile. The risk assessment process should include ongoing analysis of existing risks as well as the identification of new or emerging risks. Risks should be captured from all organisational units. ~~that originate risk.~~ Concentrations associated with material risks shall likewise be factored into the risk assessment.

Paragraph 113

Consider the following revision:

Internal controls are designed, among other things, to provide reasonable assurance ~~ensure~~ that each key risk has a policy, process or other measure, ~~as well as a control to ensure that such policy, process or other measure is~~ that is being applied and that they work as intended. As such, internal controls help ~~ensure~~ provide reasonable assurance of process integrity, compliance and effectiveness. Internal controls provide reasonable assurance that financial and ~~management~~ non-financial information is reliable, timely and complete and that the bank is in compliance with its various policies and applicable laws and regulations.

Paragraph 115

Consider the following revision:

The ~~sophistication of the~~ bank's risk management infrastructure including, in particular, a sufficiently robust data, data architecture and information technology infrastructure – should be nimble, responsive and anticipatory, and keep pace with developments such as balance sheet and revenue growth; increasing complexity of the bank's business, risk configuration or operating structure; geographic expansion; mergers and acquisitions; or the introduction of new products or business lines.

Legend
~~Strikethrough.~~ Text deleted from consultative document.
Underline: Text added to the consultative document.
Underline and bold: Text added to the consultative document with emphasis.

Paragraph 117

Consider the following revision:

> Risk measurement and modelling techniques should be used in addition to, but should not replace, qualitative risk analysis and monitoring. The risk management function should keep the board and senior management apprised of the assumptions used in and potential shortcomings of the bank's risk models and analyses. This improves the ability to identify risks ~~helps ensure more complete and accurate reflection of exposures~~ and may allow quicker action to address and mitigate risks.

Paragraph 120

This is the only paragraph that mentions exception approvals, which can have significant impact on a bank's risk exposure and governance effectiveness. Consider providing more guidance on exception approvals, particularly with regard to the roles of the board and senior management.

Paragraph 121

Consider the following revision:

> Banks should have risk management and approval processes for new or expanded products or services, lines of business and markets, as well as for large and complex transactions that require significant use of resources or have hard-to-quantify risks. Banks should also have review and approval processes for outsourcing bank functions to third parties, as well as ongoing third-party evaluations.

Principle 9: Compliance

Consider addressing the role of chief compliance officer, giving it the same level of attention that is afforded to the role of chief risk officer (paragraphs 106-109).

Based on the content of this section (integrity . . . observe the spirit as well as the letter of the law . . . supporting corporate values . . . internal codes and practice guidelines . . . fair treatment of the consumer and practices raising ethical concerns), it seems that there is an assumption that "Compliance" is de facto "Compliance and Ethics." Consider whether this is a governance weakness in the banking industry. In the words of Eleanor Bloxham, CEO of The Value Alliance and Corporate Governance Alliance, ". . . While many companies today combine compliance and ethics, that is a mistake that places the board in jeopardy. Compliance relates to following the laws, which may or may not have to do with ethics. Boards need to be attuned to the fact that shoving ethics under a compliance umbrella weakens ethics and cultural oversight. In part, it is this failure to recognize the ethics function as separate and distinct that results in the low reputation scores so many companies enjoy today."[6] (*Internal Auditor* magazine, February 2011). At a minimum, consider changing this principle from "Compliance" to "Compliance and Ethics."

Add additional content (similar to first bullet under paragraph 143) that might read "ensuring that compliance reports are provided to the board without management filtering and that compliance professionals have direct access to the board or the board's audit committee." This should be consistent for internal audit and all second line of defence functions.

Paragraph 138

This paragraph addresses the concept of consideration of reputation risk for the compliance function, with which we completely agree. However, the concept of consideration of reputation risk equally applies for all

[6] *Internal Auditor,* "Too Close for Comfort," February 2011, The Institute of Internal Auditors, p.29.

second and third line of defence functions. Consider addressing this in the sections on risk management and internal audit, as well.

Principle 10: Internal audit

This principle is worded differently than the way it is addressed in the 2012 BIS paper Internal Audit in Banks. We would suggest incorporating language more similar to the language used in that paper.

In addition, this section should specifically address the role of the chief audit executive, giving it the same level of attention that is afforded to the role of chief risk officer (paragraphs 106-109).

Paragraph 142

Consider the following revision:

The board and senior management can enhance the effectiveness of the internal audit function by:

- requiring the function to independently assess the effectiveness and efficiency of the internal control, risk management and governance systems and processes;
- ensuring that the scope of internal audit is unrestricted;
- requiring internal auditors to adhere to national and international professional standards, such as those established by ~~t~~The Institute of Internal Auditors; ~~and~~
- ensuring that audit staff have skills and resources commensurate with the business activities and risks of the bank.
- recognizing the importance of internal audit processes and communicating their importance throughout the bank;
- requiring timely and effective correction of audit issues by senior management. (Note: We are suggesting moving this bullet from paragraph 143 to this paragraph, not suggesting any change in the wording)
- ensuring that the internal audit function has an internal quality assurance capability, its performance is regularly evaluated against appropriate criteria, and it is subject to an independent, external assessment at least every five years;
- requiring a periodic assessment of the bank's overall risk governance framework including, but not limited to, an assessment of:
    - the effectiveness of the risk management and compliance functions;
    - the quality of risk reporting to the board and senior management; and
    - the effectiveness of the bank's system of internal controls. (Note: We are suggesting moving this entire bullet on the assessment of the overall risk governance framework from paragraph 143 to this paragraph, not suggesting any change in the wording)

Paragraph 143

Consider the following revision:

The board and senior management should respect and promote the independence of the internal audit function by, for example:

- ensuring that the primary reporting line of the chief audit executive is to the board or audit committee, including his/her appointment, dismissal, remuneration and appraisal.

Legend
~~Strikethrough.~~ Text deleted from consultative document.
Underline: Text added to the consultative document.
Underline and bold: Text added to the consultative document with emphasis.

- ensuring that internal audit reports are provided to the board without management filtering and that the internal auditors have direct access to the board or the board's audit committee.
- requiring, where internal audit has a secondary reporting line, that this is to the chief executive officer. (consider a comply-or-explain approach to this)
- giving internal audit the right to attend or observe executive committee meetings and to have timely access to key management information.
- ~~requiring timely and effective correction of audit issues by senior management~~.
- ~~requiring a periodic assessment of the bank's overall risk governance framework including, but not limited to, an assessment of:~~
    - ~~the effectiveness of the risk management and compliance functions;~~
    - ~~the quality of risk reporting to the board and senior management; and~~
    - ~~the effectiveness of the bank's system of internal controls.~~

Consider adding an additional paragraph that reads:

> Appointment, dismissal and other changes to the chief audit executive position should be approved by the board or its audit committee.

Principle 11: Compensation

Paragraph 148

Consider the following revision:

> For employees in risk, compliance and other second line of defence control functions, as well as the third line of defence internal audit function, compensation should be determined independently of any business line overseen, and performance measures should be based principally on the achievement of their own objectives so as not to compromise their independence.