



# FIRSTRAND

## MEMO

**To** : [baselcommittee@bis.org](mailto:baselcommittee@bis.org)  
**CC** : [SARB-BANKSUP@resbank.co.za](mailto:SARB-BANKSUP@resbank.co.za)  
**From** : FirstRand Ltd - South Africa  
**Subject** : Comments on the BCBS Consultative document – The Internal Audit function in Banks  
**Date** : 23<sup>rd</sup> February 2012

---

### 1. Introduction

We have reviewed the document entitled “Consultative document - The Internal Audit function in Banks.” In this memorandum we provide you with our views and suggestions. We also take this opportunity to thank you for including FirstRand Group Internal Audit in your initiatives.

### 2. Overall Comment

The document is based on 20 principles categorised into:

- A. Supervisory expectations relevant to the internal audit function,
- B. The relationship of the supervisory authority with the internal audit function, and
- C. Supervisory assessment of the internal audit function.

We support the proposals contained within the document however we do have two key areas that we propose be addressed in the contents:

- Inclusion of the adequacy internal control, risk management and governance processes.
- Inclusion of Financial and strategic risks

Comments on this document were provided by Group Internal Audit – FirstRand as well as the Chairman of the Group Audit Committee.

### FOR FURTHER CLARITY OR DISCUSSION, PLEASE CONTACT THE CHIEF AUDIT EXECUTIVE – DETAILS BELOW

**Mrs. Jenitha John**

**Chief Audit Executive - FirstRand Group**

PO Box 786273, Sandton, 2146 South Africa

T +27 11 282 1353 C +27 82 376 3871`

e [jenitha.john@firstrand.co.za](mailto:jenitha.john@firstrand.co.za)

We refer the reader to our detailed comments below which highlights our recommendations for consideration.



### 3. Detailed Comments and Suggestions

Overview of the principles (Page 2)	
Principles relating to the supervisory expectations relevant to the internal audit function (Page 2 and 3)	
"Principle 1: An effective internal audit function independently and objectively evaluates the quality and effectiveness of a bank's internal control, risk management and governance processes....."	<b>Recommendation:</b> Change the word "quality" to read "adequacy" so that this aligns with the standards of the Institute of Internal Auditors (IIA).
Principle 13: Internal audit should both complement and assess operational management, risk management, compliance and other control functions.	<b>Recommendation:</b> Change the words "other control" to read "other assurance" as many organisations are moving towards combined assurance principles.
Principles relating to the supervisory assessment of the internal audit function (Page 3)	
"Principle 18: Supervisors should formally report all weaknesses identified in the internal audit function to the board of directors and require remedial actions."	The responsibility for the internal audit function may be delegated to the audit committee. <b>Recommendation:</b> Rather state "Supervisors should formally report all weaknesses identified in the internal audit function to the audit committee and require remedial actions. Where an audit committee is not established, or where supervisors believe that appropriate remedial action is not taking place on a timely basis, supervisors should formally report all weakness identified to the board of directors".
"Principle 19: The supervisory authority should consider the impact of its assessment of the internal audit function on its assessment of the bank's risk profile and on its own supervisory work."	<b>Recommendation:</b> Rather state "The impact of the supervisory authority assessment of the internal audit function should be taken into consideration for the overall bank's risk profile assessment as well as on the supervisor's planned work".
A. Supervisory expectations relevant to the internal audit function	
Key features of the internal audit function (Page 5)	
Paragraph 13: "The internal audit function should not be involved in designing, selecting, implementing or operating specific internal control measures. However, the independence of the internal audit function should not prevent senior management from requesting input from internal audit on matters related to risk and internal controls. "	The statement "should not be involved in designing" removes the potential for internal audit to recommend design changes to the control environment or risk and governance processes. Assurance related advisory services are permitted by the IIA standards. <b>Recommendation:</b> Rather state "The internal audit function can recommend to management however may not take the responsibility for the design, selection, implementation or operating specific internal control measures."



### Scope of activity (Page 7)

<p>Paragraph 27: “The internal audit function should evaluate:</p> <ul style="list-style-type: none"><li>• Effectiveness and efficiency of operations;</li><li>• Reliability, effectiveness and integrity of management information systems and processes (including relevance, accuracy and comprehensiveness);</li><li>• Monitoring of compliance with laws and regulations, including any requirements from supervisors (see the following sub-section for more details); and</li><li>• Safeguarding of assets.”</li></ul>	<p>The statement does not consider adequacy of design and also does not highlight strategic and financial risk considerations.</p> <p><b>Recommendation:</b> Rather state “The internal audit function should evaluate:</p> <ul style="list-style-type: none"><li>• The adequacy of governance, risk management and internal control processes;</li><li>• Effectiveness and efficiency of operations;</li><li>• Reliability, effectiveness and integrity of management and financial information systems and processes (including relevance, accuracy and comprehensiveness);</li><li>• Monitoring of compliance with laws and regulations, including any requirements from supervisors (see the following sub-section for more details); and</li><li>• Safeguarding of assets.”</li></ul>
<p>Paragraph 29: “The head of internal audit is responsible for establishing an annual internal audit plan that can be part of a multi-year plan. The plan should be based on a risk assessment (including input from senior management and the board) and should be updated at least annually....”</p>	<p>When using an integrated risk based approach, updating plans only on an annual basis may not be sufficient or may lose relevance as risks evolve continuously in an organisation.</p> <p><b>Recommendation:</b> Rather state “The head of internal audit is responsible for establishing an annual risk based internal audit plan that can be part of a multi-year plan. The plan should be adaptive to changes and emerging risks and this should form part of the quarterly feedback to the Audit Committee.”</p>

### Risk management (Page 7)

<p>Paragraph 31: “A bank’s system of risk management supports and reflects its adherence to regulatory provisions and safe and sound banking practices. Therefore, internal audit should include in its scope the following aspects of risk management:</p> <ul style="list-style-type: none"><li>• the organisation and mandates of the risk management functions including market, credit, liquidity, interest rate, operational, and legal risks....</li></ul>	<p>The adjacent statement does not consider strategic and financial risk.</p> <p><b>Recommendation:</b> Rather state “...the organisation and mandates of the risk management functions including strategic, market, credit, liquidity, interest rate, operational, financial and legal risks....”</p>
---	--



#### Regulatory and internal reporting (Page 8)

Paragraph 35: "In addition to the matters identified above, internal auditors should regularly evaluate the effectiveness of the process by which the risk and reporting functions interact to produce timely, accurate, reliable and relevant reports for both internal management and the supervisor."

The adjacent statement does not consider design of the process, i.e. adequacy.

**Recommendation:** Rather state "In addition to the matters identified above, internal auditors should regularly evaluate the adequacy and effectiveness of the process by which the risk and reporting functions interact to produce timely, accurate, reliable and relevant reports for both internal management and the supervisor."

#### B. The relationship of the supervisory authority with the internal audit function (Page 12)

Paragraph 77: "Internal audit is well placed to provide the supervisor with insight on the institution's business model including risks in the institution's business activities, processes and functions and the adequacy of the control and oversight of these risks such as:

(i) Application and effectiveness of risk management procedures and risk assessment methodologies, as applied to credit risk, market risk, liquidity risk, operational risk (including information technology and business continuity management), ....."

Strategic and financial risks have not been considered.

**Recommendation:** Rather state "...Application and effectiveness of risk management procedures and risk assessment methodologies, as applied to strategic risk, credit risk, market risk, liquidity risk, operational risk (including information technology and business continuity management), financial risk and other risks relevant to the Basel capital adequacy Pillar 2 requirements..."

#### Annex 2 - Responsibilities of a bank's audit committee (Page 19)

##### Internal control

Paragraph f: "ensuring that senior management establishes and maintains an adequate and effective internal control framework. Such framework should be designed to provide assurance in areas including reporting (financial, operational, risk)....."

Strategic risks have not been considered.

**Recommendation:** Rather state "...Such framework should be designed to provide assurance in areas including reporting (strategic, financial, operational risk), monitoring compliance with laws, regulations and internal policies, efficiency and effectiveness of operations and safeguarding of assets."