# Audit Committee Forum™

Position Paper 6

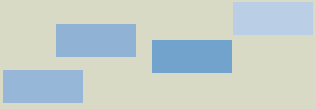
Issue Date: December 2009

**The role of the audit committee in respect of risk**

The Audit Committee Forum™ is proudly sponsored by KPMG.

# The role of the audit committee in respect of risk

*The information contained in Papers disseminated by the Audit Committee Forum™ is of a general nature and is not intended to address the circumstances of any particular individual or entity. The views and opinions of the Forum do not necessarily represent the views and opinions of KPMG, the Institute of Directors and/or individual members. Although every endeavour is made to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No reliance should be placed on these Papers, nor should any action be taken without first obtaining appropriate professional advice. The Audit Committee Forum™ shall not be liable for any loss or damage, whether direct, indirect, consequential or otherwise which may be suffered, arising from any cause in connection with anything done or not done pursuant to the information presented herein. Copyright is by the Audit Committee Forum™ extracts of this paper may only be reproduced with acknowledgement to the Audit Committee Forum™.*



# Contents

## Introduction

This paper has been revised so as to update it to take account of the implications of:

- The global financial crisis
- The King III Code and Report ("King III")
- The Companies Act, No. 71 of 2008 ("The Companies Act").

This paper is being issued ahead of the relevant effective dates[1] of the Companies Act and King III as a guideline to inform entities and afford them the opportunity to prepare themselves for these requirements.

Furthermore, there is a concern that risk governance has been focused on activities and operational issues without sufficient attention being paid to sustainability and external factors at industry, regional, national and global levels.

This paper seeks to guide audit committees in their oversight of risk management processes in order that they might be better prepared and their boards and management better equipped to address risk in all its guises.

## Risk governance structure and reporting

**The governance of risk will always remain the responsibility of the board. The board may, however, assign the oversight of risk management to an appropriate committee. There are many configurations of the structure that this delegation may take the form of in entities in South Africa.**

The board should consider the following factors in determining whether to separate or combine the audit and risk committees:

- Size of entity
- Complexity
- Type of business/industry
- Nature of risks
- Time needed to devote to risk oversight
- Ability of committee members to deal with both functions
- Legal requirements, such as the Banks Act and the PFMA.

**NOTE:** In terms of the Companies Act, 2008, the legislative requirements for the composition of the audit committee need to be taken into account when deciding to combine the audit and risk committees.

The audit committee should satisfy itself of the acceptance by the board of its own primary responsibility for the governance of all risk – both financial and non-financial risks (such as IT, operational, strategic, reputational, regulatory, sustainability, environmental and compliance risks).

When considering a suitable structure for the oversight of risk, the board should have regard to the factors outlined below.

[1] The effective dates are: King III effective 1 March 2010; Companies Act no notice of effective date yet.

## Separate audit and risk committees

**Composition:**

- An audit committee consisting of at least three independent non-executive directors, supported when necessary by expert input; and
- A risk committee consisting of executive and non-executive directors and senior members of management responsible for the various areas of risk management. The committee, taken as a whole, should comprise people with adequate risk management skills, experience and resources to ensure that the committee can perform its functions properly (supplemented by expert input when considered necessary).

**Reporting lines:**
The risk committee may report, through its chairman, either

- directly to the board (in which case the audit committee should be represented on the risk committee to provide the necessary link between the two committees so as to keep the audit committee fully informed of the financial consequences of identified risks and the management and mitigation processes and controls put in place by management); or
- to the audit committee (the Audit Committee Forum considers this to be the less preferred option in that it may diffuse the focus of the board on its risk governance responsibilities).

## Combined audit and risk committees

Combined audit and risk committees should comprise at least three independent non-executive directors. The committee should be complemented by members of executive management by invitation only (for the risk committee aspect) to ensure the relevant spread and levels of risk management skills, experience and resources to ensure that the committee can perform its functions properly (supplemented by expert input when considered necessary).

It should be noted that, in terms of the Companies Act, anyone appointed (as opposed to being invited to attend a meeting or meetings) to a board committee (including the risk committee or audit committee), where not already a director, will be a 'deemed director' with all the attendant responsibilities and liabilities, but without the right to vote unless the Memorandum of Incorporation (MOI) or a special resolution provides otherwise.

## Responsibility for risk management

**Whereas the board is responsible for the governance of risk, the Chief Executive Officer (CEO) is the executive ultimately responsible for risk management.**

The board plays a decisive role in the strategy development process and should provide input and approve the long-term and short-term strategies for the entity, ensuring that they will result in sustainable outcomes within the board's determination of the entity's risk appetite and tolerance.

Strategic planning should include an assessment of risks and opportunities and the board should satisfy itself that the strategy and business plans are not encumbered by risks that have not been thoroughly considered and quantified.

Management is accountable to the board for designing, implementing and monitoring the risk management process and implementing an appropriate risk management framework. Risks should be monitored on an ongoing basis and control activities reviewed to ensure that the controls are appropriate in responding to identified risks.

Management is also charged with ensuring that the appropriate risk assessment, response, monitoring and assurance processes are put in place by the relevant structures within the entity.

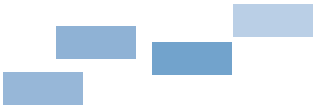
Risk awareness should be embedded throughout the entity. Everyone is responsible for considering risks that might impact on their area/sector/division of the business and the process should operate in both directions: from top down and from bottom up.

## Scope of risk

**The impact of the global financial crisis as a result of the failures of major organisations in the United States, Europe and elsewhere, has raised questions as to why the boards of those entities failed to understand or anticipate the risks inherent in their operations timeously.**

Not all risks can be mitigated and these will form part of the entity's accepted risk appetite and tolerance. The board should ensure that there is a clearly defined risk management framework which sets out the entity's appetite for and tolerance of risk. Business and strategic plans are usually reviewed annually and the review should include considering, in detail, what risks might prevent the entity from reaching or achieving any one of the objectives set out in the strategic plan.

While potentially material high-impact risks need to be assessed and plans and controls put in place to manage and mitigate them, boards should not overlook the potential impact of a combination of smaller risks occurring simultaneously and how they might be mitigated and responded to.



## Role of the audit committee in relation to risk

**Whether or not a separate risk committee has been established, the audit committee plays an integral role in the risk management process. The audit committee's primary approach to risk is to assure itself that the processes for the mitigation and management of actual or potential risks, as they relate to the audit committee's responsibilities for financial reporting, internal financial controls, fraud and IT risks (as they relate to financial reporting), are in place.**

The audit committee's charter should be clear on the scope of the audit committee's responsibilities for the oversight of the risk management function.

All risks may ultimately have a financial impact; accordingly, the potential long-term financial implications of what may be seen as non-financial risks (such as operational, strategic, reputational, regulatory, sustainability, environmental and compliance risks) cannot be ignored. Regardless of the board's method and framework for assigning oversight of the risk management function, the audit committee should have an understanding of, and an adequate level of comfort regarding, the entity's process for identifying, managing and reporting on risks which impact on financial reporting. In this regard, where a separate risk committee, reporting to the board, is appointed, the audit committee may gain this assurance by being represented on that risk committee.

Where the board assigns oversight of the risk management function to the audit committee, the audit committee's responsibility for overseeing that function should be identical to that of a risk committee in an entity where a separate risk committee is established. For this purpose, regard should be had to the principles contained in Chapter 4 of King III – The governance of risk.

Boards of entities with no separate audit or risk committees take direct responsibility for the governance of risk as well as for the oversight of the risk management function.

The audit committee should satisfy itself that the following areas have been addressed:

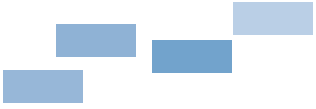
- Risk identification and assessment
- Risk management and mitigation
- Risk reporting.

## Conclusion

**The ultimate responsibility for the governance of risk rests with the board of directors. The audit committee should satisfy itself that there has been appropriate consideration of and response to those risks which impact on financial reporting, internal financial controls, fraud and IT (as they relate to financial reporting), regardless of the structures set up by the particular entity.**

For further information on risk, refer to:

| | |
|---|---|
| S94(7)(i) of Companies Act, 2008 | |
| Chapters 3 & 4 of the King III Report | **www.iodsa.co.za** |
| ISO 31000 | **www.iso.org** |
| COSO Framework | **www.coso.org** |



# Appendix A
# Risk governance structure and reporting

| Type of entity | Requirement to elect audit committee in terms of the Companies Act and King III | Responsibility for the governance of risk | Responsibility for the oversight of financial reporting risks | Structure | Reports to |
|---|---|---|---|---|---|
| **Private company without public interest** | Not required to appoint or elect audit and/or risk committees.<br><br>However, an entity which elects, in terms of its Memorandum of Incorporation (MOI), to establish an audit committee, is then bound by the Companies Act and King III.<br><br>In terms of section 34(2) of the Companies Act, these companies should determine the extent of compliance with Chapter 3 of the Act and should clearly set out the role, composition and duties of the audit committee in the MOI.<br><br>The audit committee should have at least three independent non-executive directors, elected by shareholders. | Board of directors<br><br>Board of directors | Board of directors<br><br>Audit committee | Board of directors<br><br>Either separate:<br>■ Audit committee<br>&<br>■ Risk committee<br>or<br>■ Combined audit and risk committee | Board of directors<br><br>Board of directors<br><br>Board or audit committee<br><br>Board of directors |
| **Public companies, state-owned companies, private companies with public interest** | Audit committees should have at least three independent non-executive directors, elected by shareholders. | Board of directors | Audit committee | Either separate:<br>■ Audit committee<br>&<br>■ Risk committee<br>or<br>■ Combined audit and risk committee | Board of directors<br><br>Board of directors or audit committee<br><br>Board of directors |

# Appendix B

# Previously published position papers and alerts

**These papers, prepared by the Audit Committee Forum working groups, contain guidelines for audit committee members and other interested parties.**

| Paper | Topic | Date |
|---|---|---|
| **Position Paper 1** | Guidelines for establishing a private sector audit committee | March 2008 |
| **Position Paper 2** | Guidelines on questions that an audit committee could consider before recommending an entity's financial statements for approval by the board | 2004 |
| **Position Paper 3** | Guidelines for the audit committee chair person | 2004 |
| **Position Paper 4** | Guidelines for audit committees on approving non-audit services by the external auditor | 2005 |
| **Position Paper 5** | The Corporate Laws Amendment Act, 2006 and guidance on the developing role of the audit committee | 2008 |
| **Position Paper 6** | The role of the audit committee in respect of risk | December 2009 |
| **Position Paper 7** | The internal audit function and the evaluation of its effectiveness | 2006 |
| **Position Paper 8** | The evaluation of the external auditor's audit of the financial statements | 2006 |
| **Position Paper 9** | Guidelines for assessing the performance of an audit committee | 2006 |
| **Position Paper 10** | Guidelines for the audit committee's assessment and response to the risk of fraud | 2007 |
| **Position Paper 11** | Audit committee guidelines for evaluating whistleblowing channels | 2007 |
| **Position Paper 12** | Guidelines to audit committees on Reportable Irregularities and the impact on the audit committee | 2007 |
| **Position Paper 13** | Guidelines for the audit committee's approach to Information Technology (IT) risk | 2007 |

| Alert | Topic | Date |
|---|---|---|
| **No. 1** | Audit committees top ten to do's:<br>Considerations related to the current financial crisis | March 2009 |
| **No. 2** | Establishment and membership of audit committees in terms of the new Companies Act and King III | December 2009 |
| **No. 3** | Responsibilities of the audit committee with regard to integrated reporting | December 2009 |
| **No. 4** | The audit committee's role with regard to the finance function and internal audit – King III | December 2009 |
| **No. 5** | The audit committee's role in the risk management process – King III | January 2010 |
| **No. 6** | The audit committee's role with regard to external audit | January 2010 |
| **No. 7** | The audit committee report to be included in the annual report | In progress |
| **No. 8** | The audit committee terms of reference | In progress |

## Contact details:

**Thinglemony Pather**
Director
KPMG
thingle.pather@kpmg.co.za
011 647 5037

www.acf.co.za

**Parmi Natesan**
Senior Manager
KPMG
parmi.natesan@kpmg.co.za
011 647 5963

www.acf.co.za