

# Internal audit and risk management in South Africa: adherence to guidance

First submission: 26 May 2011

Acceptance: 5 August 2011

Risk management is a relatively new addition to the wider concept of corporate governance. Sound corporate governance requires, among other things, that the board should ensure that there is an effective risk-based internal audit. The importance of internal audit within risk management and assisting the board of directors in this regard cannot be over-emphasised. The formal guidance of the IIA should be a starting point for internal auditors when performing their duties. Further applicable and comprehensive guidelines and legislation in this regard are urgently needed. This article aims to obtain input from heads of prominent internal audit functions within the private and public sectors on the role of internal auditing in the management of risk.

## Interne oudit en risikobestuur in Suid-Afrika: voldoening aan riglyne

Risikobestuur is 'n relatief nuwe ontwikkeling binne die groter konsep van korporatiewe beheer. Goeie korporatiewe beheer vereis onder andere dat 'n direksie moet verseker dat effektiewe risikogebaseerde interne oudit uitgevoer word. Die belangrikheid van interne oudit binne risikobestuur en hul rol om die direksie in dié verband by te staan, kan nie oorbeklemtoon word nie. Die formele riglyne van die IIA moet die beginpunt wees vir interne ouditeure tydens die uitvoering van hul pligte. Verdere toepaslike en omvattende riglyne hieroor word dringend benodig. Hierdie artikel het ten doel om insette van hoofde van prominente interne ouditdepartemente in die private en openbare sektore aangaande die rol van interne oudit in die bestuur van risiko te bekom.

*Dr P Coetzee, Dept of Internal Auditing, University of Pretoria, Pretoria 0001 & Prof D S Lubbe, Centre for Accounting, University of the Free State, P O Box 339, Bloemfontein 9300; E-mail: Philna.Coetzee@up.ac.za & lubbeds@ufs.ac.za.*



Risk management, a relatively new addition to the wider concept of corporate governance, has developed considerably since the introduction of the second King Report (IOD 2002) in 2002 and, in particular, since the third King Report (IOD 2009) in 2009, which requires, among other things, that the “board should ensure that there is an effective *risk based* internal audit” (own emphasis). However, since the introduction of King III organisations and the internal audit profession have not adhered to all the elements of risk management and risk-based internal audit (Castanheira *et al* 2010: 95). The development of further applicable and comprehensive guidelines and legislation in this regard are urgently needed. The recent global financial crisis highlighted the need for such guidelines and legislation. The banking sector, traditionally the leader in risk management, was very hard hit as a result of poor risk-management principles and practices (Baker 2008: 34, Lam 2009: 22). The importance of internal audit within risk management and assisting the board of directors in this regard cannot be over-emphasised. Both King Reports (2002 & 2009) recognise the importance of internal audit and risk management as cornerstones of corporate governance. The doyen of corporate governance, Mervyn King, describes internal audit as “the ringmaster in combined assurance and the right arm of the non-executive board” (Baker 2010: 31).

The majority of the parties involved in the business environment recognise that the responsibility for risk management lies with the board and senior management in private sector organisations (COSO 2004: 83-4, IOD 2009: 73), and with the accounting officer in the South African public sector (RSA 1999: S38(1)(a)(i), RSA 2003: S62(1)(c)(i)). To manage risk efficiently and effectively, management should have an understanding of the concept of risk in general and of the specific risks that threaten the organisation in particular, and should then establish a proper risk-management framework to mitigate key risks.<sup>1</sup>

Internal auditors are in the ideal position to assist management with this task. In order to perform their duties with proficiency and

1 *Cf* IOD 2002: 84, Spira & Page 2003: 643, Beasley *et al* 2005: 530, IOD 2009: 73.

due professional care (IIA 2011: 8-10),<sup>2</sup> they should have an overall understanding of how the organisation operates, as well as a sound notion of the risks threatening the organisation. They should therefore combine their broader knowledge of the business with their role of assisting management in minimising risks, while still retaining their independence from the business activities and structures.<sup>3</sup> Lubbe & Van der Merwe (2007: 25) argue that there are many reasons why risk management and internal auditing should be aligned. The most important reasons are to provide the board with an accurate risk profile; to assist internal auditing to focus on high-risk areas; to save on costs, and to improve the efficiency and effectiveness of information.

The *International Standards for the Professional Practice of Internal Auditing* (hereafter referred to as the *Standards*) and *Practice Advisories* of the Institute of Internal Auditors (IIA) (2011) address three specific areas where the internal auditor should play a role in the incorporation of risk assessment into their activities. As the formal guidance of the IIA should be a starting point for internal auditors when performing their duties, this article will focus on the following areas: the formal risk-management framework, including the risk-management process; the annual plan of the internal audit function's activities based on risk (internal audit risk assessment), and incorporating risk into individual audit engagements (risk-based internal auditing).

The objective of the article is to obtain input from heads of prominent internal audit functions (hereafter referred to as chief audit executives) within the private and public sectors on the role of internal auditing in the management of risk. This could result in providing the IIA with the necessary information to obtain insight and understanding as to what is needed to ensure that internal auditors are taking up their responsibility regarding risk management; be it to develop further guidance to assist their members, or to provide the necessary training to inform and equip members of the profession.

2 E-mail to Louw A (ane.louw@up.ac.za), 10 September 2008.

3 Cf/Spira & Page 2003: 653, IIA 2004, Fraser & Henry 2007: 406.

In order to achieve this objective, a literature review was conducted with the main purpose of investigating theoretical perspectives and previous research findings that are relevant to this article and that will guide the research in the empirical study (Leedy & Ormrod 2005: 64, Saunders *et al* 2007: 595). Formal interviews were conducted with the chief audit executives of the organisation with the highest risk maturity levels in each of the two sectors, as indicated in Coetzee's study (2010: 304-7).<sup>4</sup> The reasoning behind this decision was that if an organisation is risk mature, there is a better likelihood that internal auditing will play a more prominent role in the management of risk. Although a structured questionnaire was developed for each sector, the "descriptive method: survey research" was used to obtain quantitative primary data (Mouton 2001: 152-3). This data was collected by means of, *inter alia*, personal interviews and consisted of facts, opinions, beliefs, attitudes and behaviour (Mouton 2001: 152-3, Saunders *et al* 2007: 310). The advantages of this type of data-gathering include high confidence that the right person has responded; the likelihood that the contamination of the respondent's answers is low; the fact that open and closed questions can be included, and enhancement of the respondent's participation (Leedy & Ormrod 2005: 184-5, Saunders *et al* 2007: 354-60). This method was chosen for various reasons. First, internal auditing in the management of risk is a fairly new concept, as is evident from the studies performed in the internal audit field incorporated into the CBOOK publication (IIARF 2007: 359-405). Secondly, although internal auditors may believe that they are incorporating risk into their activities, the level of incorporation or the methodology followed may be outdated.

This article is limited by the fact that, although many books and other literature are available on this topic, the guidance discussed is limited to those provided by the IIA. Another prerequisite was that the organisations included in the article had to be risk mature, or at least examples of the highest risk-mature organisations within the specific sector. Only five organisations per sector were included. However, the risk-maturity scores for the attribute 'internal auditing'

4 Cf Appendix A for a list of the respondents from the private and public sectors.

for each of the organisations included in this study indicate that the internal audit function was risk mature, confirming that these chief audit executives were in the best position to add the most value to the study (Coetzee 2010: 314-5).

The remainder of the article addresses the three areas mentioned earlier. The review of the literature, the results of the empirical study and a conclusion will be given for each of these three areas. Lastly, a final conclusion and recommendation are provided.

## 1. Risk management

### 1.1 Background

Risk management consists of a risk-management framework, including risk-management process(es) (AS/NZS 2004: 5) that could be either comprehensive or partly implemented. The framework consists of the structures, processes and systems established by management to ensure that their risk philosophy is incorporated into the daily activities of the organisation. A risk-management process is the systematic process that is followed to identify, assess and manage risks, either on a strategic or on an operational level (Coetzee 2010: 155). The ensuing discussion refers specifically to either a risk-management framework or a risk-management process, or generally to risk management, which includes both.

### 1.2 Guidance on risk management

According to *Standard 2120* (IIA 2011: 15), the internal audit function must evaluate the effectiveness of the risk-management process. *Standard 2120.A1* (IIA 2011: 16) elaborates on this with specific reference to risk exposures relating to organisational governance, operations and information systems; *Standard 2120.A2* (IIA 2011: 15) deals with the risk of fraud, and *Standard 2120.C3* (IIA 2011: 15) provides guidance for assisting management with the establishment or improvement of a risk-management process. Various practice advisories, that are not mandatory, provide further

guidance on this topic. Although it is suggested that elements of the risk-management framework should be investigated in order to form an opinion on the adequacy of the risk-management processes, no mention is made of internal auditing being involved in the overall risk-management framework – either by providing input into the risk philosophies, risk policy, structures such as a risk committee and risk department, and the embedding of risk into the daily activities of the organisation, or providing management or the board with assurance. This is a gap in the IIA guidance on the activities of the internal audit function. Although the IIA's (2006: 14-5) position paper on corporate governance refers to the role that internal auditing should play in governance structures, including enterprise risk management as an organisational initiative impacting on governance, it does not specifically stipulate that internal auditing should be providing assurance on the effectiveness and efficiency of the risk-management framework.

The IIA (2004) issued a position paper on the role of internal auditing in risk management. The document suggests the idea of internal auditing playing a key role in providing assurance on the risk-management process, providing assurance that risks are evaluated correctly, evaluating the risk-management process, evaluating the reporting of key risks, and reviewing the management of key risks. The document distinguishes between sound internal audit practice and activities that are not appropriate for internal auditing to perform, and outlines legitimate roles that may be undertaken, but with safeguards. As with the *Standards* and Practice Advisories, although the document refers to a risk-management framework in terms of maintaining and developing it (legitimate role with safeguards), it does not include the provision of assurance under the core roles.

The second King Report (IOD 2002: 76) stipulates that an assessment of the risk-management processes in place within the organisation must be conducted on an annual basis. Internal auditing should assist in the monitoring of the processes. The third King Report (IOD 2009: 79-80, 93) elaborates on this requirement. Specific interesting additions include the reference to providing assurance on

the effectiveness of risk management (process and framework) and commenting on the level of risk maturity.

For the public sector, legislation (RSA 2003: (2)(b)(iv)) prescribes that the internal audit function in a local government organisation should advise management and report to the audit committee on the issue of risk management. Although vague, it incorporates the likely provision of assurance on the risk-management framework. The National Treasury issued an internal audit framework for all government organisations, stipulating that the internal audit function is responsible for providing assurance on the adequacy and effectiveness of risk management (RSA 2009: 21).

### 1.3 Literature review

Studies exploring the role of internal auditing with regard to risk management indicate that organisations are increasingly implementing risk management and that there is an increasing demand for internal auditing to be involved in risk management.<sup>5</sup> This involvement varies from taking responsibility for the risk-management process (not allowed according to the IIA's position paper), to auditing the risk-management process as part of the internal audit annual plan, to actively and continuously supporting and being involved in the risk-management process in a consulting role. The latter involves participation in risk committees, monitoring activities, status reporting, as well as managing and coordinating the risk-management process. However, the majority of the studies do not refer to internal auditing providing assurance on the overall risk-management framework, except for the recent study published by the IIA Research Foundation (2009) on the trends of the profession since 2009. In this study, the audit universe (IIARF 2009: 9-10) includes the overall effectiveness of risk management within

5 Cf McNamee & Selim 1998: 13, Spira & Page 2003: 656-7, Allegrini & D'Onza 2003: 198-9, Baker 2004: 17, Beasley *et al* 2005, Sarens & De Beelde 2006: 73-5, Gramling & Myers 2006: 52-8, Roffia 2007: 9, Fraser & Henry 2007: 403, Deloitte & IIA (UK and Ireland) 2008: 8, PWC 2008(a): 9, Ernst & Young 2008: 5-6, IIARF 2009: 9, Castanheira *et al* 2010: 89-94.

the organisation's risk environment, referring to both the risk-management framework and the risk-management process.

When investigating whether the activities performed by the internal audit function are in line with the guidance of the IIA, the evidence is contradictory. For example, the study by the IIA Research Foundation (Gramling & Myers 2006: 54), where 87% of the respondents indicated that they have a risk-management process in place, identifies that the core activities. According to the IIA's position paper, these are to a large extent being performed by the internal audit function. However, some of these activities (Gramling & Myers 2006: 56) contradict what the IIA suggests, such as setting the risk appetite, imposing risk-management processes and being accountable for risk management. Sarens & De Beelde (2006: 238) as well as PricewaterhouseCoopers (2007: 15) confirm this tendency. In the latter study, 32% of the respondents indicated that internal auditing is responsible for the risk-management process.

With regard to the public sector, a study done in Europe (Castanheira *et al* 2010: 92) identifies that, although internal auditing plays a proactive role in the implementation of risk management, it has no further involvement once the framework has been established. Hepworth (2004) asks the question as to whether the modern approach to internal auditing based on risk is appropriate for developing countries. He argues that the definition of internal auditing is based on the assumption that reasonable assurance can be provided. In developed countries the public sector is well structured, systems are developed and public servants are properly trained – it is thus easier for internal auditing to provide assurance. This may not always be the case in a developing country. This view is supported by Lutta & Ogwel (Baker 2005: 47) who were members of the task team assisting a Kenyan government department to develop a risk-based internal audit plan. Both stipulate that management and internal auditing must first understand the underlying concepts related to risk and risk management before a proper risk-management process can be implemented.



## 1.4 Empirical results

### 1.4.1 Background

Five areas were covered during the empirical study addressing risk management. The results and a brief discussion thereof are provided below.

### 1.4.2 Adherence to the IIA *Standards*

Table 1 provides the results for adherence to the applicable standards that reflect on risk management. It also indicates whether or not the study's respondents believed that more guidance is needed to adhere to a specific standard.

Table 1: Adherence to the IIA *Standards* related to risk management

Activity	Private sector				Public sector			
	Adherence		Guidance		Adherence		Guidance	
	Yes	No	Yes	No	Yes	No	Yes	No
IAF evaluates the effectiveness of risk management ( <i>Standard 2120</i> )	5	0	0	5	1	4	2	3
IAF contributes to the improvement of risk management ( <i>Standard 2120</i> )	5	0	0	5	1	4	2	3
IAF evaluates the risk exposure of the organisation ( <i>Standard 2120. A1</i> )	4	1	0	5	1	4	2	3

IAF – Internal audit function

For the private sector organisations only one respondent indicated that they do not fully adhere to the internal audit function evaluating their risk exposure, the reason being that certain activities are too technical and actuaries are needed to perform this task. According to

*Standard* 1210.A1 (IIA 2011: 9), this is not a valid excuse as internal auditing should contract experts when such knowledge is lacking within the internal audit function.

For the public sector, only one participating organisation adheres to the above standards with reasons for non-adherence ranging from the fact that the organisation does not have a risk-management framework in place, to the risk department being a new function and not yet fully operative. It is noted that some public sector organisations require further guidance on how to perform these tasks.

#### 1.4.2 Internal auditing’s involvement in risk management

This section investigates the risk-management activities that internal auditing could undertake. Although guidance is specific on the nature of internal auditing’s involvement, this is not necessarily the view of management and the board, and could affect the practical implementation of the risk-related activities. Table 2 provides the respondents’ points of view regarding the areas of involvement expected of the internal audit function, as guided by the IIA *Standards* and Practice Advisories.

Table 2: Areas of involvement in risk management

	Private sector	Public sector
Provide assurance on the risk-management framework	5	5
Provide assurance on the risk-management process	5	5
Participate in consulting activities	5	2
Take full/partial responsibility for implementing the risk-management framework	0	0
Taking full/partial responsibility for implementing the risk-management process	0	0

The private sector respondents’ internal audit functions include the first three areas but the respondents indicated that internal auditing can only provide input in the risk-management framework and/or process as it remains management’s responsibility to im-

plement these structures. Concerns were raised that the internal audit function lacked the resources to provide consulting activities, and should be cautious when accepting such engagements.

With regard to public sector organisations, all the respondents agreed that assurance activities should be performed, but only two agreed that internal auditing should also perform consulting activities. The reasons provided include that consulting activities should be performed by the risk department and that internal auditing should remain independent.

#### 1.4.3 Increased involvement of internal auditing

Internal auditing’s involvement in risk management has increased over the past decade mainly due to increased corporate governance legislation and guidance. Table 3 summarises the respondents’ viewpoints on whether internal auditing’s involvement in risk management has increased since 1999.

Table 3: Increased involvement in risk management

	Private sector	Public sector
Past 6 months	0	0
Past year	1	2
Past 3 years	1	1
Since Public Finance Management Act (PFMA)	N/A	0
Since second King Report (King II)	3	2
Since third King Report (King III)	0	0

For the private sector participating organisations, internal auditing’s increased involvement in risk-management activities occurred mainly due to the issuing of the second King Report (IOD 2002). Comments include the fact that internal auditing had to appoint specialists to perform certain duties; that internal auditing had first developed risk management for the organisation but since King II the function now has an assurance role to play; that internal auditing was assisting with the implementation of a risk department,

and that internal auditing recently started to develop their annual internal audit plan based on a risk assessment.

For the public sector participating organisations, risk management involvement increased mainly due to the issuing of the second King Report in 2002 or, over the past year, due to the implementation of a risk-management framework, for example, a chief risk officer has been appointed. However, not one participating respondent indicated that the PFMA influenced the internal audit function's increased involvement, even with the PFMA (RSA 1999: S38(1)) enforcing the directive that a risk assessment should be conducted and that internal auditing should use the outcome to guide their activities.

#### 1.4.4 Future increased involvement of internal auditing

The future involvement of internal auditing could be affected by certain factors such as the current global financial crisis (Coetzee 2010: 123-6). Table 4 gives the respondents' viewpoints regarding the factors affecting the potential future increase of internal auditing's involvement in risk management.

Table 4: Future increased involvement in risk management

	Private sector	Public sector
King III guidance	4	4
Current financial crisis	0	0
Board's/Executive's changed needs	2	2
Management's changed needs	1	3

The majority of the respondents in the private sector organisations were adamant that internal auditing's involvement should not increase as this could jeopardise the function's independence. However, they believed that more emphasis could be placed on the current risk-management activities performed, mainly due to the issuing of the third King Report (IOD 2009) and the board of director's changed needs. One respondent also mentioned the new Companies Act as a reason. One area that would most likely be added

to internal auditing's duties is combined assurance mapping (IOD 2009: 59). No respondents were of the opinion that the current financial crisis would influence the increased involvement of the internal audit function in risk management. This may be due to the fact that the majority of them perceive this crisis to have an effect on the global market and are unaware of how this crisis has and will affect the South African market (Van Zyl 2010: 1).

With regard to the public sector organisations' respondents, future involvement was also linked, apart from the issuing of third King Report (IOD 2009), to management's changed needs. This is mostly attributed to the fact that the risk structures are fairly new and that internal auditing's role in risk management is now entering a new dimension.

#### 1.4.5 Internal audit activities related to the risk-management framework – current and future activities

Although the IIA's position paper (IIA 2004) provides guidance to the internal audit function on the nature of its role regarding the risk-management framework, the literature indicates that the management of organisations frequently has other opinions as to what this should entail. Table 5 lists the participating organisations' activities that are currently performed, as well as the activities that are planned in terms of core or desirable activities, activities that could be performed but with caution, and activities that should be avoided at all costs. It must be noted that the activities are summarised as either consulting and/or assurance activities as this could influence whether a certain activity performed is in line with guidance or whether it is contrary to good practices.

Table 5: Current and future activities related to the risk-management framework (consulting *versus* assurance activities)

Activity	Current activity				Future activity			
	Consulting		Assurance		Consulting		Assurance	
	PR	PU	PR	PU	PR	PU	PR	PU
Core activities								
Providing assurance on the effectiveness of the risk-management framework	0	0	5	1	0	1	5	5
Evaluating the methodology of the risk-management process(es)	1	0	5	1	1	1	5	5
Evaluating the reporting of key risks	0	1	5	3	0	0	5	5
Reviewing the management of key risks	0	1	5	3	0	0	5	5
Legitimate internal audit roles with safeguards								
Facilitating the identification and assessment of risks	1	3	2	0	0	1	2	0
Coaching management in responding to risks	1	4	1	0	0	1	1	2
Coordinating organisation-wide risk-management activities	0	3	0	0	0	1	0	0
Developing the risk-management framework	0	3	1	0	0	1	1	0
Maintaining the risk-management framework	0	3	1	0	0	1	1	0
Roles internal auditing should not undertake								
Setting the risk appetite	0	0	0	0	0	0	0	0
Taking part in the risk-management process(es)	0	0	0	0	0	0	0	0
Taking decisions on risk responses	0	0	0	0	0	0	0	0
Implementing risk responses	0	0	0	0	0	0	0	0
Being accountable for risk management	0	0	0	0	0	0	0	0

PR – Private sector

PU – Public sector

It is reassuring to note that the roles which internal auditing should not undertake according to the guidance are not being performed by either sector's internal audit functions. For the private sector, the participating internal audit functions currently provide assurance on the core activities and, although some of the additional legitimate internal audit roles are being performed, organisations are planning to minimise these in the future. Public sector organisations are performing more consulting activities, probably due to the fact that risk management is relatively new in the public sector and that internal auditing is assisting management to set up the risk-management framework. This is, however, not in line with the viewpoint of chief audit executives (*cf* Table 2). According to the IIA's guidance, this is acceptable as long as internal auditing implements safeguards to ensure that their independence is not compromised. It is concluded that all the participating organisations are currently performing, or are planning to provide assurance services on core activities.

## 1.5 Conclusion

The above guidance, literature review and empirical results indicate that the role of internal auditing with regard to risk management is increasing. The IIA provides guidance to their members on the risk-management process, but not on the overall risk-management framework. However, it appears that this is an area with a new trend for internal auditing, thus guidance is needed (*cf* Table 1). In addition, although the IIA provides definitive guidance on the activities that may be performed by internal auditors *versus* what is inappropriate, studies indicate that IIA members do not always adhere to these rules. The guidance clearly stipulates the nature of assurance, consulting, and inappropriate activities. To protect their independence and objectivity, internal auditors need to follow this guidance more carefully.

With regard to the current and future involvement of the function, the private sector chief audit executives regard the second King Report as the key instigator for the increased involvement of internal auditing in risk management. King III as well as the board's changed

needs will most likely be important to guide future involvement. The current financial crisis was not mentioned, probably as a result of the view, right or not, that it has not affected the South African economy in a material way. The public sector chief audit executives indicated that the role of internal auditing within risk management has mostly evolved in the past year, with King II guidance being a major influence. It is cause for concern that the PFMA, promulgated in 1999 and addressing the role of internal auditing with regard to risk management, was not mentioned. King III and, to a lesser extent, management's and executive management's changed needs will influence the future involvement of the function.

With regard to the IIA's adherence to guidance, the public sector internal auditing functions are performing more consulting services than their private sector counterparts, probably due to internal auditing assisting management with the implementation of a risk-management framework, as indicated earlier. However, this is contrary to the views of chief audit executives that internal auditing should not participate in consulting activities regarding risk management.

## 2. Annual planning of the internal audit function's activities

### 2.1 Background

The next step for the internal auditor is to align the outcome of the risk-management process (list of risks threatening the organisation) with the activities of the internal audit function. This is also referred to as risk assessment or macro-assessment of risk.<sup>6</sup> To avoid confusion with the risk-assessment step in the risk-management process, this macro-process will be referred to as internal audit annual planning, and assessing risk as part of the process will be referred to as internal audit risk assessment.

6 Cf McNamee 1998: 71, McNamee & Selim 1998: 49-50, Allegrini & D'Onza 2003: 197, Spencer Pickett 2006: 107.



## 2.2 Guidance

The audit universe (Spencer Pickett 2006: 114-5) is a list of all possible auditable engagements that could be performed within an organisation, including both strategic and operational activities. It is generally impossible to perform all these engagements due to resource limitations. Therefore, according to *Standards* 2010 and 2010.A1 (IIA 2011: 13), the chief audit executive should base the internal audit function's plan on a risk assessment that is performed at least annually. Factors influencing this planning based on an internal audit risk assessment include, among others, components of the organisation's strategic plan, outcome of the risk-management process, and input from senior management and the board. According to the Practice Advisories (IIA 2011: 34), information obtainable through the risk-management process is crucial in developing the internal audit function's annual plan.

For South African organisations, both the private (IOD 2009: 94) and the public sector (RSA 2003: S165(2)(a), 2005: 3.2.7 & 2009(b): 17) stipulate that the internal audit function must prepare a strategic audit plan based on its assessment of key risk areas for the organisation.

## 2.3 Literature review

More internal audit functions are using risk methodologies to plan their activities and it appears that this tendency is increasing.<sup>7</sup> If a formal risk-management process is in place within the organisation, it is important for the internal audit function to consider the output of such a process in drawing up the annual plan. For example, does the annual plan cover the strategic high-risk areas to be audited within the foreseeable future (Spencer Pickett 2006: 7, PWC 2008(a): 16-8)? By using the output of the risk-management process in the planning of the internal audit function's activities, it is possible to ensure that the focus is on the most important auditable areas within the audit universe.

7 Cf Allegriani & D'Onza 2003, PWC 2008(a): 16, Castanheira *et al* 2010: 88-94, PWC 2008(b): 31.

Study results concerning the use of the risk-management process's output in the internal audit annual plan are contradictory. Some studies indicate that it is used as guidance when planning the internal audit function's activities,<sup>8</sup> while others indicate that organisations do not use this valuable source of information.<sup>9</sup> Castanheira *et al* (2010: 91-4) identify certain factors influencing the tendency to use this approach, namely the size of the organisation (larger organisations have a greater tendency), the type of industry (finance organisations tend to have the highest tendency), the sector (the private sector has a greater tendency), globalisation (international organisations have a greater tendency), and listing on a stock exchange (listed companies have a greater tendency). Of the respondents in the CBOOK study (IIARF 2007: 116), 83.7% indicated that they adhere to the guidance on how to manage the internal audit function, including the annual plan based on a risk assessment, and 28.3% (IIARF 2007: 223) indicated that they make extensive use of a specific audit tool or techniques to perform this task.

Ernst & Young's study (2007: 10) identifies a problem that could be linked to the inappropriate and ineffective planning of activities by the internal audit function. Chief audit executives worldwide indicated that they struggle to complete the internal audit annual plan – only 21% completed the entire internal audit annual plan and 24% completed up to 80% thereof – due to various reasons, including personnel shortages and not focusing on the crucial aspects identified by management. For the latter, it is vital to use internal audit risk assessment to determine these aspects.

PricewaterhouseCoopers (PWC) (2008a: 3, 16-8) highlight the importance of internal auditing focusing on strategic, operational and business risks in addition to financial and compliance risks as a new trend for the profession. The reason for this shift from the traditional focus on the latter is that 80% of loss in external shareholders' value can be linked to strategic, operational or business risks. Despite this statistic, only 24% of the Fortune 500 participants in the

8 Cf Ernst & Young 2007: 10, PWC 2007:12; PWC 2008(a):18.

9 Cf Allegrini & D'Onza 2003: 197, McCuaig 2006: 4, Arena *et al* 2006: 287, Sarens & De Beelde 2006: 76.

study (PWC 2008a: 16) indicated that the internal audit function's risk-assessment process is linked to the outcome of the risk-management process that has as its main objective to identify strategic, operational and business risks.

## 2.4 Empirical results

### 2.4.1 Background

The empirical study included two aspects that were tested, namely adherence to the IIA *Standards*, and other guidance.

#### 2.4.2 Adherence to the IIA *Standards*

Table 6 summarises the adherence levels to the *Standards* that refer to the planning of the internal audit function's activities linked to risk. The summary includes an indication of whether respondents require further guidance.

Table 6: Adherence to the IIA *Standards* related to planning the internal audit function's annual activities

Activity	Private sector				Public sector			
	Adherence		Guidance		Adherence		Guidance	
	Yes	No	Yes	No	Yes	No	Yes	No
The IAF's annual plan is risk-based, after performing an assessment ( <i>Standards</i> 2010 & 2010.A1)	5	0	1	4	5	0	0	5
The IAF accepts consulting engagements to improve risk management ( <i>Standard</i> 2010.C1)	2	3	2	3	4	1	0	5

IAF – Internal audit function

It is concluded that the overall results are in line with the literature discussed earlier – the participating organisations have a risk-based annual plan in place as drawn up by the internal audit function, but the function does not perform consulting services to improve risk management.

The private sector organisations' respondents suggested that more guidance is needed to perform these tasks. Reasons for non-adherence to the consulting activities range from the fact that the internal audit function only performs assurance services, the function does not have enough employees and/or expertise, and the risk department is providing sufficient improvement to the risk-management framework.

The public sector respondents did not express a need for further guidance. They indicated that the risk structure of the organisation is capable of providing this service but, where needed, the internal audit function will accept consulting engagements to assist the risk structure in improving risk management.

#### 2.4.3 Adherence to other guidance

As discussed earlier, the internal audit function's first step in incorporating risk-related aspects into their activities is planning the internal audit functions' annual plan using a risk assessment. For South African organisations, guidance exists for both the private and the public sectors' internal audit functions on how to establish the functions' annual plans. Table 7 indicates adherence to this guidance by the participating organisation and when implementation will occur if an organisation has not yet implemented the guidance. King III guidance is used for both sectors, with the PFMA being applicable to the public sector only.

Table 7: Adherence to guidance related to the risk-based planning of the internal audit function's annual plan

Activity	Private sector		Public sector	
	Adherence		Adherence	
	Yes	No	Yes	No
King III guidance				
Plan based on a risk and opportunities assessment performed (key risk areas)	5	0	5	0
Plan based on risks identified by management	5	0	5	0
Plan based on opportunities identified by management	4	1(*)	3	2
Plan aligned with the results of the risk-management process(es)	5	0	4	1
PFMA				
Current operations taken into account	N/A	N/A	5	0
Proposed operations in the organisation's strategic plan taken into account	N/A	N/A	5	0
Risk-management strategy of the organisation taken into account	N/A	N/A	3	2

(\*) – Implementation will never occur

For the private sector, all the participating organisations perform a risk assessment in order to develop the internal audit annual plan, which includes the identification of risks by management. However, one organisation did not include the identification of opportunities by management as part of the process and indicated that this will never occur.

Participating public sector internal audit functions perform risk assessments when developing their annual plan, including the identification of risks by management. Again, it is concluded that not all of the organisations base their plans on the opportunities identified by management or even align the plans with the results of the risk-management process. In addition, it appears that two of the organisations are not adhering in full to the public sector legislation. This is cause for concern as the PFMA was promulgated in 1999.

## 2.5 Conclusion

The literature review reveals that a properly structured internal audit risk assessment, incorporating the outcome of the risk-management process, can be used to assist the internal audit function in allocating scarce resources to investigate the strategic high-risk areas of the organisation. The empirical study's results indicate that all the organisations' internal audit functions base their annual plans on a risk assessment, incorporating the risks identified by management. However, the loss of opportunity as a risk is not always included. Although mostly adhering to the guidance on this topic, public sector organisations do not always adhere to the PFMA guidance. Respondents indicated the lack of resources as the factor that hindered full adherence the most.

## 3 Internal audit engagements

### 3.1 Background

Risk-based internal auditing expands on the processes of risk management and internal audit risk assessment by shifting the vision of an internal audit engagement. When performing an internal audit engagement, instead of assessing the business activities within the framework of the internal control system ('control paradigm'), the business activities are viewed within a framework of risk ('risk paradigm'). The internal auditor's focus moves from identifying and testing internal controls to the manner in which management addresses and manages risks – this could include internal controls. In addition, the internal auditor should, while performing the preliminary investigation of the internal audit engagement, or during the performance of the engagement, identify additional risks that are threatening the organisation's ability to achieve its objectives. In this way, internal auditing, true to the definition of the profession, could add more value in ensuring that the organisation's objectives and

goals are met, thus also assisting management. This is directly in line with sound corporate governance practice. In the literature risk-based internal audit engagements are often referred to as risk assessments or micro-risk assessments.<sup>10</sup> In order not to confuse this risk assessment with the risk assessment step in the risk-management process, as well as internal audit risk assessment as discussed earlier, this will be referred to as an internal audit risk-based engagement or, when referring to the risk assessment, as an internal audit engagement risk assessment.

### 3.2 Guidance

According to *Standards* 2200, 2201 and 2210.A1 (IIA 2011: 16-7), when planning an internal audit engagement, internal auditors must consider the significant risks to the activity under review, as well as the adequacy and effectiveness of the risk-management process(es) residing within the scope of the engagement. Practice Advisory 2210.A1-1 (IIA 2011: 74) elaborates on this by identifying certain tasks that the internal auditor should perform, such as considering the risk assessment performed on the activity under review as part of the risk-management process. If needed, the internal auditor should perform a survey to obtain information on the activities, risks and controls. Practice Advisory 2200-2 (IIA 2011: 71) also refers to a risk-based internal audit engagement, emphasising the fact that internal auditors should identify the key controls mitigating the significant risks of the organisation as a whole, instead of only the risks affecting the activity under review.

Scant guidance is available on this topic in South Africa. The third King Report (IOD 2009: 94-5) includes risk-based internal auditing concepts as a lengthy addition to the second report. It urges the internal audit function to take note of the organisation's assessment of strategic, financial, operational, compliance and sustainability risks when performing its annual planning. Although it does not specifically mention risk-based internal audit engagements, it could be assumed, by implication, that the guidance also refers to

10 Cf McNamee 1998: 71, McNamee & Selim 1998: 103, Allegrini & D'Onza 2003: 198, Spencer Pickett 2006: 143, Castanheira *et al* 2010: 79.

risk being included in the execution of an engagement. According to the Treasury Regulations (RSA 2005: 3.2.6 & 2009: 24), all internal audit engagements in public sector organisations must be performed according to the IIA's *Standards*, thus including risk-based internal auditing.

### 3.3 Literature review

After a comprehensive search, it appears that hardly any research information is available on the performance of a risk-based internal audit engagement. According to Allegrini & D'Onza (2003: 198), many internal auditors still follow the control paradigm and as such do not regard including the identification of risks when planning the audit engagement as crucial (only 67% of the respondents perform some form of risk-based internal audit engagements). This is echoed in a study by Castanheira *et al* (2010: 95), with only 31% of the respondents indicating that they take a risk-based approach during an internal audit engagement. The study by PWC (2008a: 4-5) suggests that the audit committee is setting higher performance standards for internal auditing. This includes shorter audit cycle times (from the commencement to completion of an audit engagement) due to the rapid changes within the business environment. The follow-up study (PWC 2008b: 34-5) on the future of the profession emphasises this fact by urging internal auditors to move beyond a cyclical and static audit approach and to conduct internal audit engagements on a more targeted basis responding to specific risk concerns. Focusing mainly on the high-risk areas within a specific engagement should shorten the audit cycle time as fewer audit procedures will be performed (for example, low-risk areas could be excluded). A study by Deloitte (2005: 9) among 800 executive members on the state of their organisations' control programmes complements the move to a risk-based internal audit engagement approach. With regard to the control programme in their respective organisations, 56.3% indicated that over-controlling in routine areas is cause for concern, 29.1% indicated insufficient controls in high-risk



areas, and 32.2% indicated insufficient focus on high-risk areas in audit programmes. Only 13.9% indicated that their control programmes are lean and balanced. The Practice Advisory (IIA 2011: 36) supports this by suggesting that internal auditors should identify unnecessary, redundant, excessive or complex controls that do not mitigate risk effectively and efficiently.

Various studies and other literature based on risk and the external audit profession define risk-based auditing as an audit where the efforts are focused on areas of higher risks.<sup>11</sup> They all urge external auditors to make use of this methodology, arguing that a new way of thinking is needed following all the corporate scandals where auditors have been involved. In order to achieve its objectives and goals, the organisation must address the higher risk areas which are, in general, the most crucial. Thus, by using this type of audit methodology, both the client and the external audit firm should benefit. This could be the same scenario for the internal audit profession.

## 3.4 Empirical results

### 3.4.1 Background

Although it was found that information is limited, this remains one of the areas that will have to receive more attention in the future in order to improve internal auditing's risk-related competencies and mindset as well as enabling the function to be more effective and efficient in adding value to the organisation. Therefore, the empirical study only investigated adherence to the IIA *Standards*.

### 3.4.2 Adherence to the IIA *Standards*

Table 8 summarises the results of the participating organisations' adherence to the related *Standards* and whether more guidance is needed.

11 Cf Curtis & Turley 2006, Knechel 2006, Prinsloo 2008.

Table 8: Adherence to IIA *Standards* related to the performance of risk-based internal auditing engagements

Activity	Private sector				Public sector			
	Adherence		Guidance		Adherence		Guidance	
	Yes	No	Yes	No	Yes	No	Yes	No
Consider the significant risks ( <i>Standard 2201</i> )	5	0	1	4	5	0	0	5
Consider how risk is kept to acceptable levels ( <i>Standard 2201</i> )	5	0	1	4	5	0	0	5
Consider adequacy of relevant risk-management process ( <i>Standard 2201</i> )	5	0	1	4	4	1	0	5
Consider effectiveness of relevant risk-management process ( <i>Standard 2201</i> )	5	0	1	4	4	1	0	5
Perform risk assessment to determine engagement's objectives ( <i>Standard 2210.A1</i> )	4	1	1	4	4	1	0	5

For the private sector, the respondents were of the opinion that risk-based internal audit engagements are performed, with only one organisation confirming that no risk assessment is performed. The respondents' risk departments perform this task, and their internal audit functions use the outcome of this process to determine their engagement objectives. One respondent indicated that further guidance is needed on this topic apart from the guidance in the *Standards* and Practice Advisories.

Apart from one participating public sector respondent indicating that no risk-management process exists within the organisation, the respondents were of the opinion that risk-based internal audit engagements are performed. One respondent indicated that the internal audit functions do not perform a risk assessment as this task is performed by the risk department.

### 3.5 Conclusion

By contrast to the research information available on the role of internal auditing in risk management and the incorporation of risk into the internal audit function's annual plan, relatively little information is available on the performance of a risk-based internal audit engagement. However, this does not mean that it is less important. Studies on the current and future trends in the internal audit profession all suggest that internal auditing functions will have to improve their risk-related competencies and mindset as well as be more effective and efficient in adding value to the organisation.<sup>12</sup> One area where both of these expectations can be adhered to is the performance of risk-based internal audit engagements. The empirical results indicate that most organisations' internal audit functions do perform a risk-based internal audit engagement. However, either the organisation's risk-management process is inadequate, or internal auditing is duplicating efforts. The majority of the respondents indicated that they do consider the adequacy and effectiveness of the relevant risk-management process performed by the organisation, but also indicate that they perform a risk assessment to determine the engagement's objectives.

## 4. Final conclusions and recommendations

The results of the literature study and the three empirical studies have led to certain suggestions that should be considered by various parties.

It appears that chief audit executives are still unsure as to what exactly is expected of internal auditing with regard to the management of risk as well as the incorporation of risk into the internal audit functions' activities. The reasons could be that the differences in the terminology and methodology used by organisations, those in the IIA *Standards* and those used in the literature, are confusing to some individuals. This is also evident from the fact that the role of

12 Cf Deloitte & IIA (UK and Ireland) 2008, Ernst & Young 2008, PWC 2008(b), IIA 2009.

internal auditing in the risk-management framework is not properly addressed in the IIA guidance. The role of internal auditing regarding risk should be researched and more clearly defined.

With regard to public sector organisations, the non-adherence to legislation such as the PFMA should encourage the chief audit executives to increase their involvement in risk management. The non-adherence to the IIA *Standards* on risk-related activities, as well as the limited involvement of the internal audit function in the management of risk, should encourage the use of consultants or experts by the internal audit function. The IIA should take note that members need further guidance on how internal auditing could provide assurance on the risk-management framework and on the performance of a risk-based internal audit engagement. Although respondents are of the opinion that they do adhere to the IIA *Standards*, when asked about specific activities with regard to risk management, many of the specific standards, which are compulsory, are not understood and/or adhered to.

## Bibliography

- ALLEGRIANI M & G D'ONZA  
2003. Internal auditing and risk assessment in large Italian companies: an empirical survey. *International Journal of Auditing* 7: 191-208.
- ARENA M, M ARNABOLDI & G AZZONE  
2006. Internal audit in Italian organisations: a multiple case study. *Managerial Auditing Journal* 21(3): 275-92.
- AUSTRALIAN STANDARDS BOARD AND NEW ZEALAND STANDARDS BOARD (AS/NZS)  
2004. *Risk management*. AS/NZS 4360:2004.
- BAKER N  
2008. Real world ERM. *Internal Auditor* 65(6): 32-7.  
2005. New hope for Kenya's auditors. *Internal Auditor* 62(6): 47-50.  
2004. Negotiating the rapids. *Internal Auditing and Business Risk* 28(10): 17-9.
- BEASLEY M S, R CLUNE & D R HERMANSON  
2005. Enterprise risk management: an empirical analysis of factors associated with the extent of implementation. *Journal of Accounting and Public Policy* 24(3): 521-31.
- CASTANHEIRA N, L L RODRIGUES & R CRAIG  
2010. Factors associated with the adoption of risk-based internal auditing. *Managerial Auditing Journal* 25(1): 79-98.
- COETZEE G P  
2010. *A risk-based audit model for internal audit engagements*. Unpubl PhD thesis in Auditing. Bloemfontein: University of the Free State.
- COMMITTEE OF SPONSORING ORGANISATIONS OF THE TREADWAY COMMISSION (COSO)  
2004. *Enterprise risk management integrated framework: executive summary*. Jersey City, NJ: Sponsoring Organisations of the Treadway Commission.
- CURTIS E & S TURLEY  
2006. The business risk audit - a longitudinal case study of an audit engagement. *Accounting, Organizations and Society*. <[http://www.sciencedirect.com/science?\\_ob=Article](http://www.sciencedirect.com/science?_ob=Article)>
- DELOITTE  
2005. *Lean and balanced: how to cut costs without compromising compliance*. <http://www.deloitte.com/dt/research/0,1015,Sid%253D7108%2526cid%253D158271,00.html>>

DELOITTE & THE INSTITUTE OF  
INTERNAL AUDITORS (UK AND  
IRELAND) (IIA)

2008. *Towards a blueprint for the internal audit profession*. London: The Institute of Internal Auditors (UK and Ireland).

ERNST & YOUNG

2008. *Escalating the role of internal audit: global internal audit survey*. <[http://www.ey.com/Global/assets.nsf/Australia-/AABS\\_GIAS\\_2008/\\$file/GIAS-08.pdf](http://www.ey.com/Global/assets.nsf/Australia-/AABS_GIAS_2008/$file/GIAS-08.pdf)>

2007. *Global internal audit survey: a current state analysis with insights into future trends and leading practices*. <[http://www.ey.com/Publication/vwLUAssets/Global\\_Internal\\_Audit\\_Survey\\_conducted\\_by\\_Ernst\\_Young/\\$FILE/EY\\_BRS\\_GlobalInternalAudit07.pdf](http://www.ey.com/Publication/vwLUAssets/Global_Internal_Audit_Survey_conducted_by_Ernst_Young/$FILE/EY_BRS_GlobalInternalAudit07.pdf)>

FRASER I & W HENRY

2007. Embedding risk management: structures and approaches. *Managerial Auditing Journal* 22(4): 392-409.

GRAMLING A A & P M MYERS

2006. Internal auditing's role in ERM. *Internal Auditor* 63(2): 52-8.

HEPWORTH N

2004. *Is the modern risk-based approach to public sector internal audit really appropriate for countries with less developed systems and less well trained public officials?* <[http://www.cipfa.org.uk/international/download/paper.](http://www.cipfa.org.uk/international/download/paper.internalaudit_hepworth-oct04.pdf)

[internalaudit\\_hepworth-oct04.pdf](http://www.cipfa.org.uk/international/download/paper.internalaudit_hepworth-oct04.pdf)>

INSTITUTE OF DIRECTORS (IOD)

2009. *King report on governance for South Africa*. Johannesburg: King Committee on Corporate Governance.

2002. *King report on corporate governance for South Africa*. Johannesburg: King Committee on Corporate Governance.

INSTITUTE OF INTERNAL AUDITORS  
(IIA), THE

2011. *International professional practices framework – South African student edition*. Altamonte Springs, FL: Institute of Internal Auditors.

2006. *IIA position paper on organisational governance: guidance to internal auditors*. <<http://www.theiia.org/guidance/additional-resources/suppressed-pdf/?serach=positionpaperorganizationalgovernance>>

2004. *IIA position statement: the role of internal auditing in enterprise-wide risk management issues*. <<http://www.theiia.org/iiaindex.cfm?act=iianews&detail=4910>>

INSTITUTE OF INTERNAL AUDITORS  
RESEARCH FOUNDATION (IIARF),  
THE

2009. *Knowledge alert: 2009 hot topics for the internal audit profession*. Global Audit Information Network. Altamonte Springs,

Coetzee & Lubbe/Internal audit and risk management in South Africa

- FL: Institute of Internal Auditors Research Foundation.
2007. *CBOK (A global summary of the common body of knowledge 2006)*. Altamonte Springs, FL: Institute of Internal Auditors Research Foundation.
- KNECHEL W R  
2006. The business risk audit: origins, obstacles and opportunities. *Accounting, Organizations and Society* 32(4-5): 383-408.
- LAM J  
2009. Key requirements for enterprise-wide risk management: lessons learned from the global financial crisis. *RMA Journal* 91(8): 22-7.
- LEEDY P D & J E ORMROD  
2005. *Practical research: planning and design*. 8th ed. Upper Saddle River, NJ: Pearson Education International.
- LUBBE J & R VAN DER MERWE  
2007. The relationship between ERM and internal audit. *Accountancy SA* June : 24-9.
- MCCUAIG B  
2006. Considering risk in audit planning. *Internal Auditing* 21(4): 3-12.
- MCNAMEE D  
1998. *Business risk assessment*. Altamonte Springs, FL: The Institute of Internal Auditors.
- MCNAMEE D & G M SELIM  
1998. *Risk management: changing the internal auditor's paradigm*. Altamonte Springs, FL: The Institute of Internal Auditors.
- MOUTON J  
2001. *How to succeed in your master's & doctoral studies: a South African guide and resource book*. Pretoria: Van Schaik.
- PRICEWATERHOUSECOOPERS (PWC)  
2008(a). *Targeting key threats and changing expectations to deliver greater value*. <[http://www.pwc.com/extweb/pwcpublishings.nsf/docid/state\\_internal\\_audit\\_profession\\_study\\_08.pdf](http://www.pwc.com/extweb/pwcpublishings.nsf/docid/state_internal_audit_profession_study_08.pdf)>
- 2008(b). *Internal audit 2012: a study examining the future of internal auditing and the potential decline of a controls-centric approach*. <[http://www.pwc.com/images/gx/eng/about/svcs/grms/PwC\\_IAS\\_2012.pdf](http://www.pwc.com/images/gx/eng/about/svcs/grms/PwC_IAS_2012.pdf)>
2007. *State of the internal audit profession study: pressures build for continual focus on risk*. <<http://www.pwc.com/extweb/pwzpublications.nsf/StateProfessionStudy2007.pdf>>
- PRINSLOO J  
2008. The development and evaluation of risk-based approaches. Unpubl MCom dissertation in Accounting. Bloemfontein: University of the Free State.

- REPUBLIC OF SOUTH AFRICA (RSA)  
2009. *Internal audit framework*. 2<sup>nd</sup> ed. Pretoria: Office of the Auditor General. National Treasury.
2003. *Local Government: Municipal Finance Management Act (MFMA), No 56 of 2003*. Pretoria: State Printer.
1999. *Public Finance Management Act (PFMA), No 1 of 1999 as amended by Act No 29 of 1999*. Pretoria: State Printer.
- ROFFIA P  
2007. *The internal auditing function in Italian listed companies: state of the art and future perspective*. Presentation at the 5<sup>th</sup> European Conference on Internal Audit and Corporate Governance, Pisa, 18-20 April: 2-16.
- SARENS G & I DE BEELDE  
2006. Internal auditors' perception about their role in risk management: a comparison between USA and Belgian companies. *Managerial Auditing Journal* 21(1): 63-80.
- SAUNDERS M, P LEWIS & A THORNHILL  
2007. *Research methods for business students*. 4<sup>th</sup> ed. Essex: Prentice Hall.
- SPENCER PICKETT K H  
2006. *Audit planning: a risk-based approach*. Edison, NJ: Wiley & Sons.
- SPIRA L F & M PAGE  
2003. Risk management: the reinvention of internal control and the changing role of internal audit. *Accounting, Auditing & Accountability Journal* 16(4): 640-61.
- VAN ZYL A  
2010. Jan en alleman besef nie hoe diep geldkrisis se gevolge lê. *Beeld, Sake* 24, 16 July: 1.