The Southern African Journal of Accountability and Auditing Research

Vol 17(1): 2015 ISSN 1028-9011

Contents of this issue:

Published by the Southern African Institute of Government Auditors

SAIGA

The Southern African Journal of Accountability and Auditing Research

Vol 17(1): 2015 ISSN 1028-9011

All correspondence and enquiries should be addressed to:

The Chairperson of the Editorial Board
SAJAAR
Southern African Institute of Government Auditors
Post Office Box 36303
0102 Menlo Park
South Africa

Tel:	[012] 362-1221
Fax:	[012] 362-1418
E-Mail:	central@saiga.co.za
Website:	www.saiga.co.za
NPO No:	045-133-NPO

The Southern African Journal of Accountability and Auditing Research (SAJAAR)

is the official scientific research journal of the
Southern African Institute of Government Auditors (SAIGA)
PO Box 36303, Menlo Park, 0102,
South Africa

As a fully independent refereed publication,
supported by international referees, listed, on the
South African Department of Higher Education and
Training's list of accredited journals,
it aims to advance scholarly research and debate into
accountability and auditing related topics.

The journal supports the endeavours of the Public Finance Management Academy™ which was founded by SAIGA to provide for amongst others high quality education in topics related to public finance management, and accountability.

Depending on the contributions received, SAJAAR is an annual publication. The views expressed in SAJAAR are those of the respective authors.

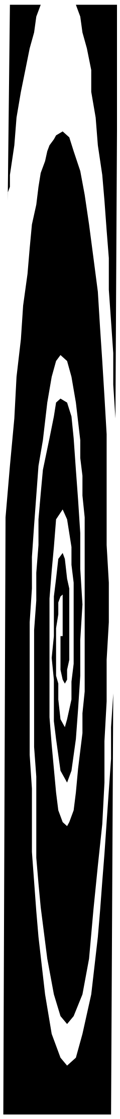
Evolving Research

The Southern African Journal of Accountability and Auditing Research

The Southern African Journal of Accountability and Auditing Research

REVIEWERS (continued)

The Southern African Journal of Accountability and Auditing Research



The SAIGA Research Award

The Southern African Institute of Government Auditors (SAIGA) has instituted an annual *Research Award*.

A panel of international experts, comprising of academics and senior government auditors make a recommendation to the Council of the Institute which makes the final decision.

It is a requirement that a nominee has to have published at least one article in *The Southern African Journal of Accountability and Auditing Research.*

The *SAIGA Research Award* is not necessarily awarded each year.

The *SAIGA Research Award* strives to encourage, support and reward independent research, discourse and contributions that advance auditing and accountability in the public sector in particular.

SAIGA

ADVANCING AUDITING AND ACCOUNTABILITY

Assessing corporate governance disclosures in South Africa's national government departments: The state and corporate governance

T Moloi

Department of Financial Governance
College of Accounting Sciences
University of South Africa

ABSTRACT

The main objective of this study is to assess corporate governance disclosures in the annual reports of South Africa's national government departments. The main finding is that national government departments do not widely adhere to sound corporate governance practices, as recommended by the King III Report on Corporate Governance, and are required by the Public Finance Management Act, and the South African Treasury Regulations. The critical areas that were poorly disclosed by national government departments include the information which indicates whether the strategic internal audit plan was based on the key areas of risk facing the department, and whether this plan had taken into account the department's risk management strategy. Further, it was not clear whether departments had Chief Risk Officers, or a directorate for risk management, to drive the risk management programme.

The study does note, however, that there are some national government departments that have demonstrated compliance with the spirit of good corporate governance by disclosing the required information in their annual reports. Stemming from this, the study recommends that those government departments which are compliant with the required corporate governance disclosures share their corporate governance disclosure practices with their counterparts in interdepartmental meetings. A further recommendation stemming from the findings is that those employees who are responsible for preparing the annual reports in each national government department should conduct a benchmarking exercise against other departments' annual reports, to assist them to identify and understand any shortcomings in their annual reports.

Key words

Annual reports; corporate governance; disclosures; integrated reports; government; departments; King III; South Africa

1 INTRODUCTION

According to Berle and Means (1932), corporate governance as a formalised concept has its origins in the 19th century, and arose in response to the acceleration in separation of ownership and control, following the formation of common stock companies. From the public sector's point of view, governance is viewed as the way in which stakeholders interact with each other in order to influence the outcome of public policy (Bovaird & Loffler 2003). From Bovaird and Loffler's perspective, public sector governance is about the interaction between the state and civil society in shaping public policy.

The Organisation for Economic Cooperation and Development (OECD) (1999 & 2004) defines corporate governance as a system by which organisations are directed and controlled. This definition is extended to include the sets of procedures and the policies that need to be followed by management and other stakeholders to assist the organisation in achieving its goals. The sets of procedures and policies serve to promote accountability and transparency, which in turn reduces the temptation of self-serving opportunism, as management and employees of an organisation are exposed to the consequences of failing to adhere to the organisation's procedures and policies (OECD 1999 & 2004).

With regard to the application of corporate governance codes in South Africa's public sector, the 2002 King Report on Corporate Governance (King II) (IOD 2002) saw only limited adoption in the public service. The limited adoption of the King II report's recommendations could largely be attributable to the fact that national government departments were already struggling to comply with mandatory legislative requirements contained in the Public Finance Management Act, 1999 (Act No. 1 of 1999) (PFMA 1999) as their minimum governance requirements; additionally, the requirement to adopt the King II report's recommendations was not a legislated requirement for the public sector.

In contrast to the requirements of the King II Report (IOD 2002), the provisions of the King III Report (IOD 2009) are specifically intended to be 'applied or explained' within all economic sectors, regardless of their manner or form of incorporation or establishment; this then implies that the King III Report is as applicable to the public sector as it is to other sectors.

The applicability of King III to all economic sectors presents an ideal opportunity to assess the extent and the degree of corporate governance disclosures in South Africa's national government departments. For the purposes of this study, assessments of the extent and the degree of disclosure of corporate governance information were conducted using information extracted directly from departmental annual reports.

The use of an annual report as a tool for the extraction of government departments' information on corporate governance is supported by various other researchers. Ponnu and Ramthandin (2008) believe that the annual report's disclosure of information on corporate governance is pertinent to the stakeholders' interests. However, Skærbæk (2005) believes that annual reports are simply intended to lend legitimacy to an organisation, and are produced mainly for external readers and audiences. For Wiseman (1982), the annual report is widely recognised as the principal means for reporting on activities and communicating intentions, and has been the source for virtually all previous corporate research. Barlett and Chandler (1997) agree with Wiseman (1982) that annual reports are seen as an important device for financial communication between management and stakeholders, while nevertheless suggesting that annual reports are still neither widely read nor fully understood by their users.

2 OBJECTIVES, SCOPE AND LIMITATIONS

The objectives of this article are twofold: firstly, to provide a brief overview of corporate governance requirements in South Africa's public sector and, secondly, to assess the corporate governance disclosures in the national government departments' annual reports.

The corporate governance information for national government departments was extracted directly from 2013 departmental annual reports, which were downloaded from their respective websites. Government departments, as well as their respective websites, were sourced from the Government Communication and Information Services (GCIS), the national agency responsible for communicating with the South African public about government policies, plans, programmes, and achievements.

In order to determine corporate governance disclosures in the annual reports of South Africa's national government departments, relevant information relating to the departments was obtained from the GCIS. Annual reports of all national government departments published prior to the 2014 general elections were considered for their corporate governance disclosures. The departments surveyed for this study were:

- Agriculture, Forestry and Fisheries
- Arts and Culture
- Basic Education
- Telecommunications and Postal Services
- Cooperative Governance
- Correctional Services
- Defence and Military Veterans
- Economic Development
- Energy
- Environmental Affairs
- Communications
- Health
- Higher Education and Training
- Home Affairs
- Human Settlements
- Independent Police Investigative Directorate
- International Relations and Cooperation
- Justice and Constitutional Development
- Labour
- Mineral Resources
- The National Planning Commission
- The National School of Government
- The National Treasury
- Planning, Monitoring and Evaluation
- Public Enterprises
- Public Service and Administration
- Public Works
- Rural Development and Land Reform
- Science and Technology
- Social Development
- The SA Police Service
- The SA Revenue Services
- Small Business Development
- The State Security Agency
- Sport and Recreation South Africa
- Statistics South Africa
- Tourism
- Trade and Industry
- Traditional Affairs
- Transport
- Water and Sanitation
- Women, Children and People with Disabilities
- The Presidency

The immediate limitation of this study is that it assesses corporate governance disclosures only in the national government departments that existed prior to the 2014 general elections. Further opportunities for research arise as a result of the departments created following the 2014 elections, and by extending the research to include provincial government departments, Chapter 9 institutions (organisations established in terms of section 9 of the South African constitution), municipalities, and state owned companies.

Furthermore, this study utilises the content analysis methodology (see section 4) as the primary tool with which to extract the relevant corporate governance information from the South African national government's departmental annual reports. This method, used as an extraction tool, has its own limitations; however, researchers such as Unerman

(2000) have observed that the recent literature still supports the content analysis technique as an acceptable research method for analysing annual reports (see also: Abeysekera 2007; Barac & Moloi 2010; Brennan & Solomon 2008; Boesso & Kumar 2007). The content analysis methodology is still considered to be useful by researchers because the technique has the ability to extract information which is not explicitly presented in a quantified and structured format, but is implicit in the sources being studied.

As indicated, the sources from which information was extracted were limited to the published departmental annual reports. The decision to limit this study to annual reports was justified on the grounds that they are the most important stakeholder documents produced by an organisation on an annual basis. Any organisation committed to promoting and maintaining good corporate governance is expected to use its annual report to communicate its progress in this regard to its stakeholders and to the public in general. The annual report provides the first impression of an institution's corporate governance compliance abilities. For Savage (1998), annual reports are an important channel by which organisations can communicate with interested stakeholders. Thomas and Kenny (1996) consider annual reports to be the least costly means of communicating with stakeholders. Wilmshurst and Frost (2000) argue that usefulness of the annual report lies in the facts that it is a statutory report containing both statutory and voluntary disclosures, is produced regularly, and can be easily accessed. Finally, Savage (1998) and Savage and Cataldo (1999), find that organisations are increasingly using their annual reports to disclose information about their social actions (social responsibility programmes), and those relating to the natural environment – in other words, addressing all issues that affect the so-called triple bottom line.

The next section of this article provides an overview of corporate governance in South Africa, and is followed by a section reporting on the findings that resulted from the assessment of corporate governance disclosures in the South African national government departments' annual reports. In the final section, results are summarised, conclusions reached and recommendations made.

3 CORPORATE GOVERNANCE IN SOUTH AFRICA

3.1 Overview of corporate governance

Following the series of high-profile corporate failures of companies such as Enron and WorldCom in the United States, and Parmalat in Italy, corporate governance became a significant topic of discussion worldwide, within the public sphere as well as within specialist financial circles. As a consequence of this increased awareness, corporate governance statements have become one of the most important disclosures included in the annual reports (Moloi 2009).

In South Africa, corporate governance was formalised in 1994 by the publication of the first King Report on corporate governance (King I) (IOD 1994). Although this report focussed a huge amount of interest on South Africa's corporate governance practices, corporate governance in South Africa pre-existed the great 1994 political change. Prior to King I (IOD 1994), corporate governance in South Africa was based on the 1973 Companies Act (RSA 1973), as well as on common law principles and precedents. However, it is generally agreed that the publication of the first King Report in 1994 went beyond the requirements of the 1973 Companies Act. King I recommended greater disclosure in the annual reports of companies, thus incorporating international best corporate governance practices into South Africa's private sector corporate governance standards.

The subsequent King Reports (King II and King III) have made it their objective to ensure that corporate governance reporting in South Africa is based on the principles of fair treatment of all stakeholders, full disclosure of corporate governance statements in annual reports, and the provision of reliable and timely disclosure of information concerning the performance of an organisation.

With the publication of the third King Report (King III) (IOD 2009), which now applies to all entities regardless of manner or form of incorporation, these aforementioned objectives have been extended into the public sector. It was noted above that the 2002 King Report on Corporate Governance (King II) (IOD 2002) had, to a limited extent, been adopted by government and the public service. The limited adoption of the King II report's recommendations (IOD 2002) was largely attributable to the pre-emptive legal requirement of compliance with the Public Finance Management Act, 1999 (Act No. 1 of 1999) (PFMA 1999), as a minimum governance requirement in the public sector, while the fact that its adoption was not a legal requirement was considered to be the primary factor limiting its implementation within the private sector.

3.2 Corporate governance requirements in the public sector

During the 2010 State of the Nation Address, President Jacob Zuma committed the South African government to ensuring that there would be speedy delivery of basic services for all citizens. The president said that "the public service has to respond to the call to make this term one of faster action and improved State performance. We require excellence and hard work" (Zuma 2010).

President Zuma's address implied that government was committed to furthering accountability, integrity, and service delivery. The establishment of departments such as the National Planning Commission and the Department of Performance Management, Monitoring and Evaluation appeared to be in line with this commitment. Improving state performance so that it can provide speedy service delivery to its citizens requires sound corporate governance practices, which should be integrated into the operational processes of the various state organs. Discussions outlining the disclosure recommendations for sound governance continue below.

3.2.1 Accounting officer/board of directors

National departments do not have boards of directors. Functions normally performed by boards of directors in companies, are performed in national departments by accounting officers and their executive management teams, commonly referred to as executive committees (departmental ExCOs). Matters relating to the strategy, risk, sustainability, and performance are dealt with in terms of Treasury Regulation 5.1.1 (National Treasury 2001), which requires that the departmental strategy is approved by the executive authority. With regard to risk management, National Treasury has published a framework which articulates the enterprise risk management (ERM) requirements for national departments. Furthermore, National Treasury requires that this framework should be applied to the departmental strategy to facilitate the processes of strategic risk identification and management.

3.2.2 Audit committees

Section 76(4)(d) and section 77 of the Public Finance Management Act (PFMA 1999), read in conjunction with Treasury Regulation 3.1.8, require each departmental accounting officer to set up an independent audit committee. The committees established in terms of these regulations must operate in compliance with written terms of reference. The Public Finance Management Act requires that the audit committees meet at least twice annually, in addition to meeting with the Auditor General (AG) at least once per a calendar year.

In addition to the requirements outlined above, Treasury Regulation 3.1.8 and the PFMA require that the committee members meet annually, independently of management of the department concerned. With regard to the chairperson of the audit committee, Section 76(4)(d) and 77 of the PFMA, read together with Treasury Regulation 3.1.4, requires the chairperson to be independent, knowledgeable of the status and position for which they have been selected, and must have the requisite business, financial, and leadership skills. The selected chairperson may not be an employee of the department concerned.

Concerning the activities of the audit committee, Treasury Regulation 3.1.10(g) requires the audit committee to coordinate all assurance activities in the department, which includes the activities of internal audit, external audit, other assurance providers, and management. Additionally, Treasury Regulation 3.1.13 sets out the requirements relating to the audit committee's review of and reporting on financial controls, and on the quality of management in the institution.

With regard to risk management, Treasury Regulation 3.1.10(c) requires the audit committee to review the key areas of risk to be covered by internal and external audit. Treasury Regulation 3.2.7(a) requires that the strategic internal audit plan be based on key areas of risk facing the institution, and take into account its risk management strategy.

Treasury Regulation 3.1.9 requires each department's annual report to include a disclosure paragraph stating whether the audit committee has fulfilled its responsibilities for the year, in compliance with its terms of reference.

3.2.3 Governance of risk

With regard to the governance of risk, King III has positioned risk management as a cornerstone of governance. The concept of risk is not entirely new to the public sector, for instance the Public Sector Risk Management Framework (issued by National Treasury in 2010, had already embraced the principles contained in the second King Report on Corporate Governance (IOD 2002).

In terms of the application of risk management principles in the public sector, Section 38 (a) (i) of the PFMA makes risk management the responsibility of the department's accounting officer. In order to comply with the provisions of Section 38, the accounting officer should start by appointing a departmental risk management committee to assist in discharging these responsibilities. Through the risk management committee, the accounting officer should ensure that risks facing the department are assessed, responses to potential risks are formulated, and developing risks are monitored on an on-going basis. With regard to assurance, the internal audit function has to assess the risks facing the department and provide assurance that the existing, or proposed, risk responses are sufficient to mitigate the identified risks.

3.2.4 Governance of information technology

With regard to the governance of information management, the National Treasury Risk Management Framework encourages institutions to adhere to the principles espoused in the King II (2002) Report on Corporate Governance for the promotion of an advanced level of institutional conduct. While King II was superseded by King III in 2009, it is reasonable to assume that the principles embodied in King III will be endorsed in future revisions of the Treasury Framework, to take into account more recent developments.

The King III Report on Corporate Governance recommends that the strategic assets of IT and its related risks and constraints should be well governed and controlled, to ensure that IT supports the strategic objectives of the department. Treasury Regulation 5.2 also makes IT governance the responsibility of the accounting officer, and this should be reported on in the annual report. Furthermore, Section 38 1(a) of the PFMA makes it the duty of the accounting officer to ensure that the institution has (and maintains) effective, efficient, and transparent systems of financial, risk management, and internal controls. The accounting officer can assign this duty to a Chief Risk Officer (CRO). Having established the role of the CRO, Treasury Regulation 3.2.11 requires him/her, through the internal audit function, to evaluate the existing controls in the information systems.

3.2.5 Internal audit and control

The King III Report on Corporate Governance directs the internal audit function to address strategic, operational, financial, and sustainability issues in its quest to deliver value to the department. Furthermore, King III calls for the chief audit executive (CAE) to provide an annual assessment of the institution's control environment.

With regard to the public sector corporate governance requirement, Treasury Regulations 3.1.10(c) and 27.2.7(a) require the internal audit function to prepare a rolling three-year internal audit plan based on its assessment of key areas of risk and on the departmental strategy. Treasury Regulation 3.1.9 requires the internal audit function to report directly to the accounting officer of the relevant department. Treasury Regulation 3.1.13 requires that the department's audit committee comments on the effectiveness of the institution's internal controls in the annual report.

A further requirement of the internal audit function is set out in Section 38(a)(ii) of the PFMA: this section requires that the internal audit function be under the control and direction of the audit committee. This section of the PFMA is consistent with Treasury Regulation 3.1.10(b), which requires that the audit committee evaluates the effectiveness of the internal audit function.

3.2.6 Annual reporting and disclosure

With regard to annual reporting and disclosure requirements, Section 40 of the PFMA and Treasury Regulation 18.3 both require the department's annual report to include the standard financial statements, and additionally, a measurement of performance against predetermined objectives. The responsibility for reporting this performance against objectives rests with the accounting officer of the department concerned.

The audit committee appointed by the department's CFO is required to comment on the annual financial statements in the annual report. Treasury Regulation 3.1.13 determines that the audit committee must report on the evaluation of annual financial statements, which would include an assessment of the department's going concern/sustainability status.

4 RESEARCH METHODOLOGY

The author of this study prepared schedules of questions (checklists) intended to gauge the extent and the level of disclosure of information in government departments' annual reports pertaining to accounting officers and their decision-making philosophies, and the disclosures on audit committees, risk management, information technology governance, internal audit, and integrated reporting. The formulated checklist questions were used to code required information in national government departments' annual reports against a three-point scale from full disclosure, through partial disclosure to non-disclosure, as shown in Table 1.

In order to determine the extent and the quality of information disclosed in each section, and to decide if the department had fully disclosed, not disclosed, or only partly disclosed the required corporate governance information in its annual report, the empirical method known as content analysis was used. Content analysis can be defined as a systematic, replicable technique for compressing many words of text into fewer content categories, based on explicit rules of coding (Berelson 1952; Krippendorff 1980; Weber 1990).

According to Krippendorff (1980), there are three (3) factors that support content analysis as a suitable technique for coding information in reports, namely stability, reproducibility, and accuracy.

Table 1: Guiding principles of data extraction – the content analysis technique

	Full disclosure of recommended information	Non-disclosure of recommended information	Recommended information partly disclosed
Guiding disclosure principles	If the required information is disclosed under its category, in a paragraph, a few paragraphs, or a full page, and this information contains all the required information, as well as voluntary disclosures for that category, the item is marked as **Yes** in the checklist.	If there is no disclosure at all of the minimum required information, the item is marked as **No** in the checklist.	If the minimum required information is disclosed, but this information is not disclosed separately under its category, and is not disclosed in detail, i.e., appears in one sentence that does not give adequate details, the item is marked **Partly** in the checklist.

From the description of the content analysis technique above, it becomes clear that it enables researchers to sift through large volumes of data in a systematic fashion with relative ease (US General Accounting Office 1996). Content analysis can also be a useful technique for discovering and describing the focus of attention of individuals, groups (whether social, private and/or other special interest), and institutions (Weber 1990), while allowing inferences to be made, which can then be substantiated using other methods of data collection.

Krippendorff (1980) notes that much content analysis research is motivated by the search for techniques to infer from symbolic data information which would be too costly, no longer possible, or too obtrusive to obtain by the use of other techniques.

In order to accomplish the objectives of this article, the author formulated the set of coding guiding principles that was utilised in coding relevant information from the annual reports. These principles are presented in Table 1, above.

5 RESEARCH FINDINGS AND INTERPRETATION

During the assessment it was noted that some government departments had been reconstituted under the new administration (post 2014 elections), while other entirely new departments had been established (e.g., Small Business Development, and Telecommunications and Postal Services). By basing the assessment on the 2013 annual reports, new departments were excluded from the study. The reconstituted departments were analysed based on the manner in which they were constituted in 2013 (i.e. Traditional Affairs was previously part of Cooperative Governance, Women was previously known as Women, Children and People with Disabilities, while Water and Sanitation was previously Water Affairs).

The National Planning Commission and the Department of Planning, Monitoring and Evaluation were analyzed as part of the Department of the Presidency's annual report. All but two of the departments published their annual reports on their respective websites; the exceptions were the Department of Home Affairs and the Department of Women, Children and People with Disabilities, for which annual reports could not be located. As a result, it was not possible to analyse these two annual reports for their disclosure of corporate governance information.

The research findings, presented below, demonstrate the results of content analysis for disclosure of corporate governance information, as performed on the national government departments' annual reports.

Table 2: Accounting officer, audit committee, chair, risk and audit plans and compliance

No.	Category and disclosed item	Fully disclosed	Not disclosed	Partly disclosed	Total
Accounting officer					
1	Strategy, risk, performance and sustainability incorporated into the department's decision making philosophy	0	31	3	34
2	Department has an accounting officer	34	0	0	34
Audit committees					
2	Department had an audit committee	34	0	0	34
3	Audit committee had a charter/written terms of reference	34	0	0	34
4	Audit committee met at least twice in the 2012/13 financial year	34	0	0	34
5	Audit committee met the AG at least once in the 2012/13 financial year	28	3	3	34
6	Audit committee met at least once in the 2012/13 financial year without the department's management being present	0	34	0	34
Audit committee chair					
7	The audit committee chairperson was independent, knowledgeable of the status and position, and had the requisite business, financial, and leadership skills	13	5	16	34
8	The audit committee chairperson was not an employee of the department	21	6	7	34
Coordination of assurance activities and review of financial controls					
9	The audit committee coordinated all the assurance activities in the department, which included activities of internal audit, external audit, other assurance providers, and management	3	31	0	34
10	The audit committee reviewed and reported on financial controls and the quality of management in the department	29	3	2	34
Review of risks and internal audit plans					
11	The audit committee reviewed the key areas of risk to be covered by internal and external audit	11	18	5	34
12	The strategic internal audit plan was based on key areas of risk facing the institution, and took into account its risk management strategy	10	19	5	34
Compliance with its charter/terms of reference					
13	Annual report included a disclosure regarding whether or not the audit committee had satisfied its responsibilities for the year, in compliance with its terms of reference	32	0	2	34

Table 2 shows the categories of disclosed topics (numbered 1 to 13) that relate to the role of accounting officers, the presence of audit committees in the national government departments, the characteristics of the audit committee chairpersons, the coordination of assurance activities and review of financial controls, the review of risks and internal audit plans, and the audit committees' compliance with their respective charters or terms of reference.

With regard to compliance with the requirement that the departmental strategy, risk, performance and sustainability functions be incorporated into the department's decision-making philosophy, the researcher found that thirty one (31) national government departments did not disclose this information in their annual reports, that only three (3) departments partly disclosed this, and no (0) departments provided full disclosure. However, the analysis did show that all national government departments assessed did have accounting officers, even though some held the position in an acting capacity.

Regarding the audit committees, assessed information revealed that national government departments had enhanced disclosures. For instance, all national government departments disclosed in their annual reports that they had audit committees; that these audit committees had written terms of references, and that the audit committees met at least twice in the year under review (2013). Twenty eight (28) national government departments fully disclosed the fact that they had met with the Auditor-General (or AGSA officials) in the year under review; three (3) did not disclose this information, and the remaining three (3) partly disclosed this information. However, none of the departments’ annual reports contained information relating to whether the departmental audit committees had met without the participation of departmental officials.

With regard to the audit committee chairpersons’ disclosures, it was found that national government departments performed poorly with regard to the disclosure of information relating to the chairperson’s independence, knowledge, status, position and skills (including his/her requisite business, financial and leadership skills). To this effect, thirteen (13) departments fully disclosed, five (5) did not disclose, and sixteen (16) partly disclosed the required information. There was however an enhanced disclosure of information confirming that the audit committee chairperson was not an employee of the department: twenty one (21) national government departments fully disclosed this fact, while seven (7) partly disclosed and only six (6) did not disclose at all.

With regard to the coordination of assurance activities and the review of financial controls, it was found that twenty nine (29) national government departments fully disclosed the fact that the audit committee had reviewed and reported on financial controls and on the quality of management in the department, while two (2) partly disclosed this information and three (3) did not disclose this information at all. In contrast, the coordination of assurance activities by the audit committees of departments was found to be poorly disclosed. In this regard, thirty one (31) national government departments’ annual reports did not contain any information on the role of audit committees in coordinating assurance activities, while three (3) national government departments fully disclosed the required information.

Table 3: Risk, information management, internal audit and integrated reporting

No.	Category and disclosed item	Fully disclosed	Not disclosed	Partly disclosed	Total
Governance of risks					
1	Risk management is a responsibility of accounting officer	15	19	0	34
2	Department has a risk management committee	20	12	2	34
3	Risks are assessed, risk responses formulated, and monitored on an on-going basis	3	10	21	34
4	The internal audit function has assessed the departmental risks, and provided assurance that risk responses are sufficient to mitigate the identified risks	3	23	8	34
5	The department has a Chief Risk Officer (CRO	5	28	1	34
Information management					
6	IT governance is the responsibility of the accounting officer	0	30	4	34
7	The fact that IT governance is the responsibility of accounting officer is reported in the annual report	0	30	4	34
8	The duty of the accounting officer is to ensure that the institution has and maintains effective, efficient, and transparent systems of financial, risk management, and internal control	0	30	4	34
9	The internal audit function evaluates the controls in the information systems	6	26	2	34
Internal audit					
10	The internal audit address strategic, operational, financial and sustainability issues	5	24	5	34
11	The chief audit executive (CAE) provides an annual assessment of an institution’s control environment	0	34	0	34
12	The internal audit function has prepared a rolling three-year internal audit plan, based on its assessment of key areas of risk and the departmental strategy	9	22	3	34
13	The internal audit function reports directly to the accounting officer of the relevant department	11	22	1	34
14	The internal audit function is under the control and direction of the audit committee	5	27	2	34
15	The audit committee evaluates the effectiveness of the internal audit function	23	10	1	34
16	The department’s audit committee comments on the effectiveness of the institution’s internal control in the annual report	32	2	0	34
Integrated reporting					
17	The annual report of the department reports on performance against predetermined objectives, in addition to the standard financial statements	34	0	0	34
18	The audit committee reports on the evaluation of annual financial statements, which includes an assessment of the department’s going concern/sustainability status	32	1	1	34

There was poor disclosure by national government departments of information relating to the review of risks and audit plans by the audit committee. Regarding this topic, nineteen (19) government departments did not disclose the information relating to the review of key areas of risk to be covered by internal and external audits in their annual reports, while eleven (11) fully disclosed this information, and five (5) partly disclosed this information. Similarly, ten (10) national government departments fully disclosed that their strategic internal audit plan was based on key areas of risk facing the institution and that they had taken into account its risk management strategy, while nineteen (19) did not disclose this information, and five (5) partly disclosed this information.

Table 3 shows the categories and disclosed topics (numbered 1 to 18) relating to the governance of risk, governance of information technology, role of internal auditing and integrated reporting.

In assessing corporate governance disclosures in the annual report, this researcher found that the disclosure of information relating to the governance of risk in national departments was generally weak. For instance, of the thirty four (34) assessed annual reports, only five (5) indicated that they had either a Chief Risk Officer or a directorate for risk management. The information relating to the assessment of risk, formulation of responses to risk, and monitoring of risks, was also poorly disclosed, with twenty one (21) national government departments partly disclosing this information, while ten (10) departments did not disclose this information at all. On a similar note, the information regarding the provision of assurance by internal audit functions that the risk responses are sufficient to mitigate risks was poorly disclosed, as only three (3) national government departments disclosed this information in their annual reports. By contrast, information relating to the departmental risk management committees demonstrated better disclosure practices, as twenty (20) national government departments fully disclosed in their annual reports that they had risk management committees.

With regard to the governance of information technology, all items relating to this topic were poorly disclosed in the assessed annual reports. This was consistent with the recurring observation made during the analysis, where audit committees highlighted information technology as a high risk area in national government departments, and that the extent of this risk could be attributable to capacity limitations or a lack of skills within the departments. The outcome of this analysis was consistent with the poor disclosure regarding the responsibilities of accounting officers in the national government departments regarding IT systems. Similarly, the roles of internal auditors in ensuring that the controls relating to the proper evaluation of information systems were also poorly disclosed.

Another disclosure element that was missing from the annual reports of the national government departments related to the role of internal auditors. National government departments' reports contained little information relating to the role of internal audit in addressing strategic, operational, financial, and sustainability issues. The annual reports also failed to provide complete information on internal audits' annual assessment of the institutions' control environments (usually provided by the Chief Audit Executive), nor did they adequately address the preparation of a three (3) year rolling plan based on the key areas of risk, the review of departmental strategy by internal audit, nor the lines of reporting of internal audit functions.

An improved level of disclosure was however observed in the information relating to the activities of the audit committees. For instance, twenty three (23) national government departments disclosed the fact that their audit committees had evaluated the effectiveness of the internal audit function, while only ten (10) did not disclose this information, and one (1) partly disclosed the required information. The information relating to comments by the audit committee in the annual report on the effectiveness of their institution's internal controls also demonstrated a high level of disclosure, as thirty two (32) national government departments disclosed this fact. Only two (2) departments did not disclose this information.

With regard to disclosure of information relating to their performance against predetermined objectives, national government departments demonstrated a high level of disclosure. Similarly gratifyingly, thirty two (32) national government departments' annual reports contained information relating to the report of the audit committee on the evaluation of annual financial statements, which also included an assessment of the department's going concern/ sustainability status.

6 CONCLUSION AND AREAS FOR FUTURE RESEARCH

In conclusion, the study found that national government departments do not demonstrate significant adherence to sound corporate governance practises (as recommended by the King III Report on Corporate Governance, the Public Finance Management Act, and the Treasury's Regulations), in respect of disclosures in their annual reports. Areas of concern include the lack of disclosures of information relating to the incorporation of departmental strategy, risk, performance, and sustainability into the department's decision-making philosophy; the meeting of the departmental audit committees in the absence of the department's officials; the audit committee chairperson's independence, knowledge of the status of the position, and possession of the requisite business, financial and leadership skills; the coordination of assurance activities by the departmental audit committees, and the review of risk management and audit plans by the audit committee.

Further areas of concern include the lack of disclosures on the following: information indicating whether the strategic internal audit plan was based on key areas of risk facing the institution and had taken into account its risk management strategy; indications as to whether departments had either a Chief Risk Officer or a directorate for risk management; the assessment of risk, formulation of responses to risk, as well monitoring of risk; the provision of assurance, by the internal audit function, that the risk responses were sufficient to mitigate risks; governance and control of information technology; the role of internal audit in addressing strategic, operational, financial and sustainability issues; the provision of an annual assessment of the institution's control environment by the Chief Audit Executive; internal audit's preparation of a three (3) year rolling plan based on the key areas of risk and the departmental strategy, and lastly, internal audit functions' lines of reporting.

The less-than-complete disclosure of required and recommended information, with no supporting explanations, in the national government departmental annual reports, casts doubt on the true state of corporate governance in government departments. This could be symptomatic of inherent challenges, such as the lack of skills or capacity to handle the governance programme. There are however some national government departments which did demonstrate the spirit of good corporate governance by disclosing the required information in their annual reports.

It is therefore recommended that those government departments which are already complying with statutory and recommended corporate governance practices share their experiences and expertise with their less compliant counterparts in specifically convened meetings, or as add-ons to regular intra-governmental (interdepartmental) meetings. Additionally, this study's findings suggest that those officials who have the responsibility of preparing the annual reports in each department should conduct a benchmarking exercise against other departments' annual reports, in order to understand what might be missing from their own annual reports.

This study assesses corporate governance disclosures in the national government departments at the end of the 2013 reporting period (i.e., prior to the 2014 elections). Annual reports from departments created after the 2014 election, as well as provincial government departments, Chapter 9 institutions, municipalities and state owned companies, were not analysed and therefore present opportunities for future research. Undertaking research on these state institutions will provide a holistic picture of the level of the state's compliance with good corporate governance practices.

REFERENCES

Abeysekera, I. 2007. Intellectual capital reporting between a developing and developed nation. *Journal of Intellectual Capital*, 8(2):329-345.

Barac, K. & Moloi, T. 2010. Assessment of corporate governance reporting in the annual reports of South African listed companies. *The South African Journal of Accountability and Auditing Research*, 10(1):19-28.

Bartlett, S.A. & Chandler, R.A. 1997. The corporate report and the private shareholder: Lee and Tweedie, Twenty Years On. *British Accounting Review*, 30:1-21.

Berle, A. & Means, C. 1932. *The Modern Corporation and the Private Property*. New York: Harcourt, Brace and World.

Berelson, B. 1952. *Content Analysis in Communication Research*. Glencoe, Illinois: Free Press.

Boesso, G. & Kumar, K. 2007. Drivers of corporate voluntarily disclosure: A framework and empirical evidence from Italy and the United States. *Accounting, Auditing and Accountability Journal,* 20(2):269-296.

Bovaird, T & Loffler, E. 2003. *Public Management and Governance*. New York: Routledge

Brennan, N. & Solomon, J. 2008. Corporate governance, accountability and mechanisms of accountability: An overview. *Accounting, Auditing & Accountability*, 21(7):885-906.

Institute of Directors (IoD). 1994. *King Report on Corporate Governance for South Africa*. Johannesburg: IOD.

Institute of Directors (IoD). 2002. *King Report on Corporate Governance for South Africa*. Johannesburg: IOD.

Krippendorff, K. 1980. *Content Analysis: An Introduction to its Methodology*. Newbury Park CA: Sage.

Institute of Directors (IoD). 2009. *King Report on Corporate Governance for South Africa.* Institute of Directors in Southern Africa: Johannesburg.

Moloi, S.T.M. 2009. *Assessment of Corporate Governance Reporting in the Annual Reports of South African Listed Companies*. University of South Africa: Pretoria.

National Treasury. 2001. *Treasury's Regulations*. Pretoria: South Africa

Organisation for Economic Cooperation and Development (OECD). 1999. *Principles of Corporate Governance*. Paris: OECD.

Organisation for Economic Cooperation and Development (OECD). 2004. *Principles of Corporate Governance*. Paris: OECD.

Ponnu, C.H. & Ramthandin, S. 2008. Governance and performance: publically listed companies in Malaysia. *Journal of Business Systems, Governance and Ethics*, 3(1):35-53.

Republic of South Africa. 1973. *Companies Amendment Act No.61, 1973.* [Online]. http://www.acts.co.za/company/index.htm. (Accessed: 10/07/2014).

Republic of South Africa. 1999. *The Public Finance Management Act No.1, 19991973.* [Online]. http://www.treasury.gov.za/legislation/PFMA/act.pdf (Accessed: 8 July 2014).

Savage, A. 1998. *Environmental Disclosures in Annual Reports. A Legitimacy Theory Framework*. Presented at an American Accounting Association Conference, USA.

Savage, A. & Cataldo, A.J. 1999. *A Multi-Case Investigation of Environmental Legitimation in Annual Reports.* Presented at an American Accounting Association Conference, USA.

Skærbæk, P. 2005. Annual reports as interaction devices: the hidden constructions of mediated communication. *Financial Accountability & Management*, 21(4):385-411.

Thomas, P.B. & Kenny, S.Y. 1996. *An Exploratory Study of the Extent of the Environmental Disclosures by Multinational Corporations*. Unpublished Paper, USA: Middle Tennessee State University and University of Utah.

Unerman, J. 2000. Methodological issues – Reflections on quantification in corporate social reporting content analysis. *Accounting, Auditing & Accountability Journal*, 13(5):667-681.

US General Accounting Office. 1996. *Content Analysis: A Methodology for Structuring and Analyzing Written Material.* GAO/PEMD-10.3.1: Washington DC.

Weber, R.P. 1990. *Basic Content Analysis*. 2nd edition. California: Newbury Park.

Wilmshurst, T.D. & Frost, G.R. 2000. Corporate environmental reporting: A test of Legitimacy theory. *Accounting, Auditing and Accountability Journal*, 13(1):10-26.

Wiseman, J. 1982. An evaluation of environmental disclosures made in corporate annual reports. *Journal of Accounting, Organisation and Society*, 7(1):53-63.

Zuma, J. 2010. *State of the Nation Address by His Excellency JG Zuma, President of the Republic of South Africa; Joint Sitting of Parliament, Cape Town*. [Online]. http://www.thepresidency.gov.za/pebble.asp?relid=211 (Accessed: 11 July 2014).

Addressing emerging risks in transborder cloud computing and the protection of personal information: The role of internal auditors

T Banda Jangara
Department of Auditing
University of Pretoria

H Bezuidenhout
Department of Auditing
University of Pretoria

ABSTRACT

There is general consensus amongst researchers that most South African companies are not yet ready to comply with the Protection of Personal Information Act No. 4 of 2013 (the POPI Act) as they lack the necessary skills, knowledge and understanding to effect such compliance. Whilst the flow of personal information to trans border clouds is lawful according to section 72 of the POPI Act, and cloud services offer benefits such as cost savings and agility, it has been determined that companies are yet to take cognisance of the fact that there are risks associated with such transfers. Five preeminent emerging risks associated with cloud data storage include data location, security, privacy, legal compliance and the cloud service providers themselves. Because of their role as assurance providers, with knowledge about organisational strategy, processes and operations, internal auditors are found to be uniquely positioned within companies to assist effectively with risk management as required by The Institute of Internal Auditors' *International Standards for the Professional Practice of Internal Auditing* and the corporate governance standards presented in King III. Internal auditors have been shown to be able to assist in mitigating each of the five emerging risks through their effective auditing of contracts, policies, procedures and controls, which ultimately results in effective advice and assurance for boards, management and stakeholders.

Key words

Cloud computing; internal auditing; personal information; risk management; transborder

1 INTRODUCTION AND BACKGROUND

Today, it is common knowledge that there are certain risks associated with the transfer of personal information by organisations to transborder clouds (European Commission 2012:5; Fischer 2012:5). Moreover, the mismanagement of personal information can have very serious consequences for organisations that collect personal data as part of their business processes. In 2008, the South African subsidiary of Zurich Insurance experienced a data leak during a routine transfer of data to a data storage centre, resulting in the loss of the personal information of 46 000 clients. The company was subsequently fined £2.3 million by the United Kingdom Financial Services Authority (FSA). The FSA stated that Zurich Insurance had failed to oversee the service provider that had been entrusted with the management of the information, and that it should have had full control of the process, despite the outsourcing arrangement (BBC News 2010). In another incident, Sony reportedly lost $171 million after a cyber-attack that resulted in 77 million accounts (complete with customers' personal information, including names, logins, passwords, emails addresses and credit card numbers), being compromised in 2011. British regulators subsequently fined Sony £250 000 for failing to prevent the cyber-attack (AON South Africa 2012; CBS News 2013). These are just two examples of many cited in the media, where personal information that is under the control of companies has been compromised. South African companies must take cognisance of the fact that without adequate protection, personal information may be lost, leaked and exposed to misuse, with negative and potentially damaging consequences.

In South Africa, the latest King Report on Corporate Governance (King III) issued by the Institute of Directors in Southern Africa (IOD 2009) gives guidance on what constitutes good corporate governance for all legal entities (Walker & Meiring 2010; Marks 2010). Chapter 4 of King III (IOD 2009:73) states that the governance of risk is the responsibility of the board of directors and is of paramount importance in conducting business. Because information is viewed as a business asset, the protection of personal information is one of the King III recommendations (IOD 2009; IT Governance

Network 2010). Boards of directors in companies want the assurance that all data or information management risks have been identified and mitigated, where necessary. Internal auditors can assist with fulfilling this requirement through risk identification and assessments, identification of the correct risk responses, continuous monitoring and the provision of assurance (in the form of formal reports on their analyses of situations) (IOD 2009:73, 93; Telavance 2012).

Information technology (IT) governance is the focus of Chapter 5 of King III (IOD 2009:82). Companies need to ensure that their IT infrastructures and business procedures enhance their abilities to achieve their business goals. In this regard, cloud computing is a technology that holds great benefits, especially for information management, but in order to be effective its inherent risks must be identified and managed (IT Governance Network 2010; AbuOliem 2013:521-522). IT should be treated as an integral part of organisation-wide risk management processes, with the integrity and security of information and privacy needing to be managed effectively (IOD 2009:85-86; IT Governance Network 2010). Compromising security and privacy are two of the five emerging risks inherent in the transfer of personal information to transborder clouds.

When it becomes operational in 2016, the Protection of Personal Information Act No. 4 of 2013 (the POPI Act) will have an impact on virtually every area of business, as it introduces a new and stringent personal information management standard with which companies will have to comply (IT Governance Network 2010). This will then put South Africa on par with other countries that have enacted and implemented data protection legislation (Liston 2012: 15; Wehler 2013). Moreover, failure to comply with the POPI Act, as well as any kind of data loss, can result in mandatory fines, similar in magnitude to those described above; this is in addition to the reputational damage organisations might suffer from the negative publicity relating to the loss of customers' personal information (the POPI Act at section 107; PwC 2012:2-4; Lamprecht 2013; Wehler 2013). Section 19 of the POPI Act makes it clear that organisations are responsible for securing the personal information that is entrusted to them by data subjects. The section states that this must be done by taking measures to identify and address risks relating to the management of personal information.

An area of business on which the POPI Act will have an impact, and of which internal auditors need to aware, is the transborder flow of personal information to the cloud (Kafouris 2014). IT is an industry characterised by rapid advances in both software and hardware innovation, and where trends emerge, experience wide-spread adoption and change rapidly. In a recent KPMG survey, 59% of the participants agreed that cloud computing is not going to be a short-lived fad; in fact, it represents the present and future of IT (Chung & Hermans 2010:16). In 2010 it was estimated that by 2014, cloud computing would be an industry worth $148 billion (Gartner 2010). Many organisations in South Africa have already migrated their IT operations to the cloud, and many more are currently in the process of doing so. The use of cloud solutions, many of which are located outside the country, is also increasing in South Africa (Bortz 2011a).

Whilst the transfer of personal information to foreign-based clouds is allowed in terms of section 72 of the POPI Act, organisations have to take cognisance of the fact that there are risks associated with the transfer of data, which are outside their control. This is because outside service providers are used, and they are domiciled in (and subject to the legal systems of) foreign territories (Watson 2013; De Stadler 2013b). In addition to the security and privacy risks, there are also the risks associated with the diminution (or even complete loss) of control over the information that is entrusted to cloud service providers; and there is a potential conflict between South African law and the laws on data protection in the territories to which the information has been transferred (Bortz 2011b; Chan, Leung & Pili 2012:4).

The *International Standards for the Professional Practice of Internal Auditing* (IIA Standards 2013) state that internal auditors must know about information technology governance and risks and risk management processes, and have the skills necessary to conduct technology-related audits (IIA Standards 2013: 1210.A3; 2110.A2; 2120.A3). Internal auditors can therefore be expected to provide their companies with guidance on identifying and mitigating the risks associated with the transfer of personal information to transborder clouds (CIIA UK 2014:1; IIA Dallas 2012:14-15; Protiviti 2012:3). In order to provide adequate protection for personal information when transferring it to transborder clouds, five risks need to be addressed. Addressing these risks can form the basis on which internal auditors can build comprehensive audit plans and provide management with risk management advice and assurance for personal information flows to transborder cloud solutions. These risks relate to:

1 data location;
2 security;
3 privacy;
4 legal compliance; and
5 cloud service providers (Chan *et al* 2012:1-22; European Commission 2012:5-24; Hahn, Askelson & Stiles 2006:1-23; New Zealand Government 2009:8-38; Protiviti 2012:2).

Because these are emerging risks, there is a heightened need for effective risk management, and good corporate governance dictates that the internal audit function plays an active part in risk management (IOD 2009:93; IIA Standards 2013: 2110.A3). Internal auditors can assist companies with the identification and mitigation of these risks because they are uniquely positioned, both by training and position within corporate structures, to provide assurance and consulting services to companies. As noted previously, and repeated here because of its seriousness, failure to adequately manage the personal information that is transferred to a cloud service provider outside South Africa can result in severe penalties against and reputational damage to organisations (PwC 2012:2-5; Kafouris 2014).

The objectives of this research are therefore:

- to introduce cloud computing as a technology which has benefits for companies, while also highlighting the fact that it carries inherent risks that need to be addressed if it is going to be used successfully;
- to highlight the impact of the POPI Act on the management of personal information in South Africa by summarising the requirements of section 72 of the Act;
- to explain the crucial role of internal auditors in evaluating risk; and
- to give insight into the role that internal auditors can play in providing companies with assurance that the five risks identified above can be managed.

2 VALUE OF RESEARCH

Chan *et al* (2012:1), predicted that the use of cloud computing solutions would increase drastically in 2014. Currently (this research was conducted in April 2014), 50% of companies in South Africa already use cloud solutions, and growth at 16% per year is being forecast (Speckman 2014). With this anticipated growth, it is imperative that companies understand how to legally transfer personal information to the cloud, while simultaneously ensuring that the associated risks are identified and managed.

Organisations are at varying stages of maturity in their efforts to comply with the POPI Act. There is a broad consensus amongst authors of articles published in the general circulation media and gathered during informal discussions, that most organisations are not yet ready to manage the risks already present when dealing with personal information, nor are they able to comply with the POPI Act; it appears that they indeed lack the necessary skills, knowledge and understanding to effect such compliance (Dlamini 2013; Lamprecht 2013; Kolver 2014; Phakathi 2014).

This research is important because, in the light of the immanent implementation of the POPI Act, the progress made in the protection of personal information by South African companies is inadequate to create the requisite internal governance frameworks, from a risk management and compliance perspective, that are necessary for the optimal and legal use of transborder cloud computing services (Bortz 2012; Senathipathi, Chitra, Angeline Rubella & Suganya 2013:2712). The internal auditing profession can and must play a pivotal role in assisting to mitigate the risks associated with the transfer of personal information to transborder clouds. This research will contribute to the body of work that companies and internal auditors can draw on in their efforts to address these important tasks.

3 RESEARCH METHOD AND LIMITATIONS

The research methodology used in preparing this article is a literature review. This research explores a relatively new area which is at the intersection of technological, legal and internal auditing issues. The research is limited to the review and analysis of legislation in the areas of personal information protection, cloud computing, and the transborder flow of personal information, an overview of internal auditing in the academic arena, and the review of professional journals and opinion pieces by industry players.

4 LITERATURE REVIEW

4.1 Cloud computing

4.1.1 Introduction to cloud computing

Cloud computing provides an internet-based system of shared resources, software and information, all of which is available on demand. The systems are managed by service providers who are responsible for the necessary infrastructure, and this allows organisations to avoid the cost of owning and managing their own IT facilities and staff (Krutz & Vines 2010:3-6; Wolfe 2011:599). Cloud computing is considered a “new technology” because some of the advantages and risks that it introduces into the IT arena are new (Von Solms & Viljoen 2012:73).

There are three cloud service delivery models (Infrastructure as a Service ‘IaaS’, Software as a Service ‘Saas’, and Platform as a Service ‘Paas’), and four deployment models (private cloud, public cloud, community cloud and hybrid cloud) (Hon, Hornle & Millard 2011:3; Noltes 2011:7-11). For the purposes of this research, the distinction between these models will not be considered.

While 50% of South African companies use cloud computing solutions, and a further 16% intended to start doing so in 2014, there is an even greater projected growth in cloud computing use in the rest of Africa: 44% of Nigerian companies and 24% of Kenyan companies report that they will begin to make use of the cloud “soon” (Speckman 2014). Despite this actual and projected growth, a survey by Portio Research revealed that more than 50% of IT decision-makers apparently know very little about cloud computing (Hsu 2012:14). As custodians of the personal information provided to them by customers, organisations (their directors and management) remain ultimately responsible for the protection of that information, even if it is transferred to a foreign-based cloud (IOD 2009:82-87; Tomaszewski 2013:3).

4.1.2 Advantages of cloud computing

Cloud computing’s advantages include its ability to provide flexible and universal access to IT resources (both software and hardware infrastructure), and the fact that costs can be charged to customers on the basis of actual use (Hon *et al* 2011:3). The benefits of using the cloud, which make it so attractive to organisations, include the following:

- *Cost management* Organisations are able to determine what IT services they require without having to spend capital on (almost instantly obsolete) infrastructure. They can also pay for services as and when required, as opposed to entering into long-term, binding enterprise agreements preferred by local suppliers.

- *Agility in sourcing and deploying services* This has become possible because solutions are already housed in the cloud, and do not need to be rolled out into IT systems housed on organisations' premises.

- *Availability* Services are usually uninterrupted because the cloud is internet-based and thus borderless and free of operational work-day and work-shift considerations.

- *Scalability* Cloud services can be adjusted almost instantly to accommodate varying levels of demand; this can assist organisations in controlling costs.

- *Increased efficiency* Because IT management is outsourced to cloud service providers IT departments can then focus on core skills and drive innovation for business development.

- *Resilience* In the face of cyber-attacks and any type of denial-of-service event, the cloud provides almost unlimited disaster-recovery options, including mirrored data centres in multiple locations (Krutz & Vines 2010:4-10; Bilton 2011; Chan *et al* 2012:3).

4.1.3 Transborder cloud computing

According to a Deloitte and ITWeb survey, 56% of South African organisations stated that they did not transfer information across the borders of South Africa. Most of them, however, used third parties to provide them with cloud computing solutions, and thus had no idea of their data's ultimate destination, or where it was managed or stored (Chivers & Kelly 2012). The probability is that their information is being transferred outside the country, without their knowledge, as many servers are housed internationally (Kafouris 2011; Chivers & Kelly 2012). The strict and onerous requirements contained in the POPI Act do not tolerate this lack of knowledge of the ultimate storage place of personal information that organisations hold. To be able to ensure the protection of information, companies have to be aware of where it is. They also need to be fully aware of what transborder clouds are and the implications of using them because the risk inherent in the use of cloud solutions for personal information rests with organisations, regardless of where their service providers transfer the data (AbuOliem 2013:522).

4.1.4 Classification of information and the risks associated with cloud computing

According to AbuOliem (2013:521), "[c]loud computing is only attractive if it embodies the principles on privacy and data ownership". It has to be accepted that there are risks associated with the transfer of data to the cloud. Information is valuable and attacks on information technology systems continue to increase in criminal efforts to gain access to information (Fowler 2003:1). During a discussion held at Microsoft's South African offices in February 2014, Watson explained that for security purposes, before organisations make use of cloud solutions, they must go through a process of classifying information, as making use of the cloud inevitably involves some loss of control; information is often transferred off the organisation's premises and subsequently managed by cloud service providers.

The classification of information involves its categorisation according to its critical value to the organisation, and the safeguards that are necessary to ensure information confidentiality, integrity and availability (Fowler 2003:3; Hahn *et al* 2006:17). By classifying information, organisations can show how they arrive at the decisions they make for managing information, including what technology is used to process it, how it is transferred, and how it is protected (Fowler 2003:3; Hahn *et al* 2006:17). For the purpose of this research, the process of information classification will not be explored. It is sufficient to state that by classifying information, the decision to transfer it to the cloud can be critically considered in the light of the risks to which it will be exposed, and the consequences that will follow if the risks materialise.

Some of the risks that have to be explored by organisations when considering adoption of the cloud include the following:

- loss of control over the information by data subjects (providers of personal information) and the organisations which collect it;

- limited or no access to information by data subjects when it is required;

- loss of privacy and security, as cloud service providers may have access to the information;

- the threat of cyber-attacks and the consequent compromising of information;

- challenges in controlling costs: verifying that what is charged for services is commensurate with what is actually being provided;

- jurisdictional conflicts with cloud servers' host countries, where data protection and privacy laws are incompatible or non-existent; and

- difficulties in mounting challenges in the event that information security is breached (Hurwitz, Bloor, Kaufman & Halper 2009; New Zealand Government 2009:4-28).

4.1.5 Cloud computing and internal auditing

As mentioned previously, cloud computing is a technology whose use is projected to increase (Chan *et al* 2012:1; Speckman 2014). Internal audit professionals need to be aware of the advantages and of the risks associated with the use of technologies such as cloud solutions (IIA Dallas 2012:9; Protiviti 2012:3; Sammut 2013). Internal audit is well positioned as an assurance provider to assist company boards and management to identify the key risks that are inherent in the use of cloud solutions (Protiviti 2012:3) To address the impact of cloud computing on the company's risk profile, internal audit has to shift its focus from traditional IT processes and procurements, to include risks specific to this technology (Sammut 2013).

In accordance with the IIA Standards (2013: 1210.A.3 & 2120.A1) and corporate governance standards such as those presented in Chapter 7 of King III (IOD 2009), the internal audit function can, and ultimately must help the business to identify, assess and mitigate the risks associated with cloud computing, in order to ensure that business benefits are realised. Slater (2012:7) believes that in addition to auditing the cloud solutions and cloud service providers so that companies engage appropriate services, internal auditors can also play a crucial role in ensuring that the company has in place adequate security and legal compliance frameworks to mitigate the chances of risk realisation (IIA 2004:203; Hahn *et al* 2006:1; IIA Standards 2013: 2110.A2; Grant Thornton 2014).

4.1.6 The protection of personal information in cloud computing

In most organisations information has become their most valuable asset and resource (Fick 2010:22). Accordingly, it has to be treated with the same, if not a higher, level of care as the organisation's financial assets. This involves the preparation and implementation of adequate information governance measures (Fick 2010:22). Nevertheless, using cloud computing for processing and storing personal information raises serious data management risks (European Commission 2012:5; Fischer 2012:5). According to Bortz (2011a), the biggest risk organisations have to contend with when placing personal information in the cloud is the protection of data and privacy.

Many organisations have failed to pay appropriate attention to data protection in cloud solutions (Fischer 2012:34). In the cloud, information is often managed by cloud service providers, and is not fully controlled and/or monitored by the companies that gather the data. This means that there is diminished control over who can access information and who can use it. Protecting intellectual property and safeguarding employee, customer and third party data have therefore become key challenges. If any form of information management risk is realised, with personal information being illegally accessed and used, there are serious legal, financial and reputational repercussions for companies (Hsu 2012:14; PwC 2012:4; Kafouris 2014). In addition, the requirements of the POPI Act hold serious implications for the users of cloud solutions (Bortz 2011b). Persons, both natural and juristic, need the assurance that their personal information is protected, regardless of the jurisdiction in which it is housed. Hence, companies that gather the data have to adhere to the conditions stipulated by data protection laws, including the POPI Act (Fischer 2012; Kafouris 2014).

4.2 The Protection of Personal Information Act 4 of 2013 (POPI Act)

4.2.1 Introduction to the POPI Act

The POPI Act was signed into law in November 2013. Its enactment established a new and higher standard to which organisations need to adhere when managing personal information. The definition of 'personal information' is found in Chapter 1 of the POPI Act, and covers a broad spectrum of personally identifiable information categories. It also specifically extends protection to the personal information of juristic persons (De Stadler 2013b; Wehler 2013).

The purpose of the POPI Act is clearly stated in section 2 of the Act. It is to protect personal information by giving effect to the right to privacy, while balancing this against other rights such as the right of access to information. It also recognises that there needs to be regulatory guidance for the free flow and use of personal information for legitimate local and international objectives, such as the provision of services and business processes (Kuner 2011:10; Gardner 2012). The Act is designed to provide assurance that natural and juristic persons' personal information will be subject to rigorous controls when being collected, transferred, stored, secured and used by organisations, thereby minimising the opportunities for inadvertent and/or negligent disclosure and misuse (Dlamini 2013; Wehler 2013).

This new law aligns South Africa's data privacy and protection legislation with international best practice. Having been modelled on the EU's Data Protection Directive 95/46/EC (EU Directive), the POPI Act is Africa's first comprehensive data and information protection law (Wehler 2013). However, it does differ in some respects from the EU Directive. Firstly, the EU Directive deals with 'data' in general (which includes personal information), while the POPI Act focuses specifically on personal information. Given its South African focus, for the purpose of this research, data therefore refers to personal information (Fischer 2012:36; Watson 2013). It is also important to note that the definition of personal information contained in the Act includes juristic persons, whereas the EU Directive limits its scope to natural persons (Dhont & Woodcock 2014).

Chapter 3 (Part A) of the POPI Act provides eight "*Conditions for Lawful Processing of Personal Information*", the operational essence of the Act. When these are complied with and implemented fully, they provide protection for personal information, and by complying with the Act, organisations (responsible parties) avoid prosecution and possible penalties (Gardner 2012; O'Donoghue 2013).

Section 19 is part of Condition 7 (Security Safeguards) of Chapter 3 of the POPI Act, and sets out what the Act requires in terms of securing personal information to ensure its integrity and confidentiality. According to section 19(1), when personal information is under an organisation's control, the organisation is obliged to take all necessary technical and organisational measures to prevent any kind of loss, damage or unlawful access that may result in the information and the data subjects who supply the information, being compromised. Section 19 (2) goes on to state that:

19. (2) In order to give effect to subsection (1), the responsible party must take reasonable measures to-

(a) identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control;

(b) establish and maintain appropriate safeguards against the risks identified;
(c) regularly verify that the safeguards are effectively implemented; and
(d) ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.

This section, together with King III's (IOD 2009) recommendations on corporate governance standards, and the IIA's Standards (2013: 1210.A3, 2120.A1) on information technology risk management, collectively form the basis on which this research is premised, in that it focuses on the management of risks associated with the transborder flows of personal information to the cloud.

An organisations' failure to comply with the POPI Act, and its failure to protect the personal information in their possession or that they have control over, must be reported to the Regulator. The consequences of such a failure can result in any of the following penalties:

- significant reputational damage;
- loss of customer confidence and business;
- imprisonment for between 12 months and 10 years (section 107 of POPI);
- fines of up to R10 million (section 109 of POPI); and/or
- civil action which could be instituted by individuals or in the form of a class action (Gardner 2012; O'Donoghue 2013; Kafouris 2014).

4.2.2 The impact of POPI on the work of the internal auditing profession

The POPI Act affects every area of business because all organisations have to ensure that all personal data is managed in accordance with its parameters (IT Governance Network 2010). In this rapidly changing regulatory and business environment, internal audit needs to find new ways to deploy its risk- and control-based skills to help the company to achieve its strategic objectives and to facilitate value creation (CIIA UK 2014:2; Ernest & Young 2011:4; KPMG 2008:6-7). This includes being able to assist with management of risk pertaining to personal information. An important role that the internal audit function plays is to provide "advice to management on governance risks and controls, for example, the controls that will be needed when undertaking new business ventures" (The Institute of Chartered Accountants in England and Wales (ICAEW) 2004:3). The introduction of the POPI Act can be considered as having engineered a new venture which will have an impact on the way in which companies conduct their business.

Internal auditors have to be qualified and skilled in the operations of the businesses they serve (CIIA UK 2014:1). Besides providing guidance for the effective implementation of the controls outlined in the POPI Act, internal auditors also need to be able to test (during their audits) the efficacy of policies, processes, controls and risk mitigation steps that organisations' management teams have put in place in order to comply with the Act (Grant Thornton 2014). In addition to being familiar with the positive controls and requirements within the POPI Act, internal auditors must simultaneously understand the severity of the consequences of failing to comply with the POPI Act (Hahn *et al* 2006:1-2; Grant Thornton 2014).

4.2.3 The POPI Act and transborder flows of personal information: section 72

Information and technology have rendered the world borderless in terms of the flow of data. There are legal benefits to these advances in information flow as countries have been forced to develop effective data protection and privacy legislation (Hahn *et al* 2006:1; Kuner 2011:24). Because of the global nature of these information flows, territories are also harmonising their legislation to ensure that information can flow unhindered between countries with similar legislation (Kuner 2011:24). South Africa has recognised that harmonising its legislation with existing international laws is crucial; hence the inclusion of Section 72 in the POPI Act, which specifically regulates transborder information flows (Watson 2013; De Stadler 2013b). Quoting from the POPI Act:

TRANSBORDER INFORMATION FLOWS

Transfers of personal information outside Republic

72. (1) A responsible party in the Republic may not transfer personal information about a data subject to a third party who is in a foreign country unless-

(a) the third party who is the recipient of the information is subject to a law, binding corporate rules or binding agreement which provide an adequate level of protection that-
(i) effectively upholds principles for reasonable processing of the information that are substantially similar to the conditions for the lawful processing of personal information relating to a data subject who is a natural person and, where applicable, a juristic person; and
(ii) includes provisions, that are substantially similar to this section, relating to the further transfer of personal information from the recipient to third parties who are in a foreign country;

(b) the data subject consents to the transfer;

(c) the transfer is necessary for the performance of a contract between the data subject and the responsible party, or for the implementation of pre-contractual measures taken in response to the data subject's request;

(d) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the responsible party and a third party; or

(e) the transfer is for the benefit of the data subject, and-
(i) it is not reasonably practicable to obtain the consent of the data subject to that transfer; and

(ii) if it were reasonably practicable to obtain such consent, the data subject would be likely to give it.

4.2.4 Application of section 72 to transborder cloud computing solutions

The POPI Act contains certain provisions that have a direct impact on the use of foreign-based cloud solutions. Some of these provisions are found in section 72 (Bortz 2011b; Watson 2013). This section provides a good balance between the protection of personal information while simultaneously recognising the importance of the unhindered transfer of that information both out of and into the Republic, for legitimate business purposes (Watson 2013). This is beneficial for South African organisations that make use of foreign-based cloud computing solutions (Pieters 2013), and for the cloud computing service providers who transfer clients' personal information abroad for processing, management and storage (Wehler 2013).

Under section 72(1) (a), organisations are now obliged to establish what data protection laws exist in the jurisdictions to which they want to transfer personal information (Bortz 2011b). There must thus be assurance that the level of data protection in the jurisdiction where the cloud's hardware and management reside is at least comparable to the requirements of the POPI Act (Fischer 2012). If no comparable law exists, organisations can make use of Binding Corporate Rules (BCRs), which ensure that a high level of protection is afforded to personal data in an organisation. These would need to be comparable to standards set by the POPI Act (Bortz 2012).

4.3 Internal auditors and risk management: transfer of personal information flows to the transborder cloud

The role of internal audit in private organisations is to provide independent assurance that risk management, governance and internal control processes for information management are in place and operating effectively (CIIA UK 2014). Slater (2012:2) adds that internal auditors also have the task of ensuring that companies will meet the requirements to pass external audits.

4.3.1 Strategic positioning of internal auditors in companies

Chapter 7 of the King III report (IOD 2009) stresses that the internal audit function in companies not only assesses controls, but goes further and assists with risk management processes (Marks 2010). This includes the management of risks faced by the personal information that companies collect and use in the course of their business (IT Governance Network 2010). Internal auditors can and must play a pivotal role in assisting organisations to ensure that they adequately protect personal information when it is transferred to transborder clouds (PwC 2011:1-2; Protiviti 2012:3).

Internal auditors, through a combination of assurance and consulting, assist organisations to achieve their goals (CIIA UK 2014:1). Internal auditors are uniquely positioned within organisations, fulfilling their role as independent advisors by maintaining a thorough knowledge about their organisation's strategy, processes and operations (ICAEW 2004:1-2; CIIA UK 2014:1). The multidimensional nature of the internal auditor's role lends credence to the assertion that through effective internal auditing, the risks that are associated with the transborder flows of personal information to the cloud can be identified and effectively managed. Internal auditors have the following advantages over normal line and staff functions in that they have

- access to management whom they can independently advise;
- access to international best practice through organisations such as the Institute of Internal Auditors (IIA);
- an in-depth understanding of organisational structure, strategy and operations;
- skills to assess policies, processes and procedures, and the ability to test their efficacy;
- the ability to identify fraud, and to control shortfalls and inherent risks; and
- the critical knowledge to recommend controls to mitigate risk and to ensure compliance (Hahn *et al* 2006:1, 17-25; Protiviti 2012:3; CIIA UK 2014).

Barac and Coetzee (2012:36) state that there is an increasing demand for internal auditors who have the skills and ability to identify and advise on the mitigation of business risks, and that there is currently a lack of such specialisation in areas such as information technology, information management and risk management. In order to assist their organisations effectively, internal auditors need to add to their abilities by continually enhancing their skills and in-depth knowledge about the risks associated with personal information management and cloud computing, as is required by the IIA Standards (2013: 2120.A1; 1210.A3).

4.3.2 Risk management process: the role of internal auditors

The National Institute of Standards and Technology (NIST) defines risk as "a function of the likelihood of a given threat-source's exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization" (Noltes 2011:23). The likelihood of a future negative event occurring is considered by assessing how often similar threats to an IT system have occurred, as well as the system's potential vulnerabilities. Impact refers to the extent of harm that could be caused to the organisation by the exploitation of identified vulnerabilities. Accordingly, risk is measured as the product of 'likelihood' and 'impact' (Noltes 2011:23).

According to the IIA Standards (2013), internal auditors must "evaluate the effectiveness and contribute to the improvement of risk management processes" (IIA Standards 2013: 2120:A1). With the passing of the POPI Act, internal auditors face a new and exacting challenge in dealing with data protection in South Africa. According to PwC (2012), "[k]eeping the audit committees of their organisations appraised of emerging risks and effective ways to address them is a key role of internal audit". The IIA Standards (2013) state that internal auditors must have the necessary proficiency and expertise to identify key information technology risks, and the skills and procedures to perform appropriate audits (IIA Standards 2013: 1210:A3).

Internal auditors also need to ensure that threats to information technology are fully considered and that the necessary policies, procedures and controls are in place so that organisations comply with legislative and corporate governance requirements (IIA Standards 2013: 1210.A3 & 2120.A2; PwC 2012:8; IOD 2009: 93). In order to accurately inform the audit committee about emerging information technology risks and how to mitigate them, it is important for internal auditors to understand the information technology governance systems of their organisations. They can then assess the effectiveness of the systems in furthering the objectives of the organisations (IIA Standards 2013: 2110.A2).

Internal auditors can play an effective risk management role by effecting the following:

a *Risk identification, assessment and analysis*. The internal audit function assists companies to identify and assess the risks they might face in achieving their business objectives. Internal audit also helps assess the likelihood of the risk being realized, and the probable impact thereof, helping to prioritize management attention by ranking risks in terms of their potential severity.

b *Controls evaluation and remediation*. The internal audit function can assess whether the institution's controls, which include the policies and procedures they have put in place, are adequate to mitigate the identified risks.

c *Regulatory compliance*. Regulatory compliance risk has greatly increased due to increasing number of statutory and regulatory frameworks that must be complied with. These include the King III report (IOD 2009), the new (2008) Companies Act, and now the POPI Act. A culture of compliance can enhance an organization's risk maturity through ongoing internal audit assessment and associated remediation efforts.

d *Improved process effectiveness and efficiency*. Internal audit can also help to enhance the effectiveness and efficiency of continuous assessment processes, and to identify any shortcomings in the methodology used to complete tasks.

e *Assurance to the board, management and other stakeholders*. Internal audit provides assurance that companies have governance frameworks that effectively mitigate the various risks they face, and that contribute to meeting business objectives (Telavance 2012; Ernest & Young 2011:5-6; PwC 2011; Chan *et al* 2012:4-6, 17-20; CIIA UK 2014:1-2).

4.4 Five emerging risks inherent in the transfer of personal information to the transborder cloud, and the associated role of the internal auditor

Nicolaou, Nicolaou and Nicolaou (2012) state that companies must be able to audit their cloud services in order to assess the adequacy of controls for risks that are inherent in the use of cloud technology. It is axiomatic that knowledge of these risks is critical in that it enables internal auditors to audit a cloud computing solution properly, and thereby to add value to their organisations (Nicolaou *et al* 2012). Five emerging risks require analysis, understanding and effective management if personal information is going to be transferred to the transborder cloud in a manner that is compliant with the requirements of section 72 of the POPI Act. These risks are or relate to the following:

1 data location;
2 security;
3 privacy;
4 legal compliance; and
5 cloud service providers (Chan *et al* 2012:1-22; EU Commission 2012:5-24; Hahn *et al* 2006:1-23; New Zealand Government 2009:8-38).

Internal auditors can provide assurance that the management of such risks is appropriate by being aware of the risks associated with the use of this technology, and by assisting in the mitigation of such risks through ongoing assessments and audits (IIA Dallas 2012:9; Protiviti 2012:2). To ensure the security of personal information and compliance with legislative requirements (including those of the POPI Act), specific risks should be proactively identified, understood and management protocols developed prior to making use of cloud services (Protiviti 2012:6; Bortz 2011b). It is essential that internal audit participates in the process from the initial stages of cloud technology implementation, and before the "live" personal information is transferred to the cloud. Failure to do this invites the possibility that the associated risks will be realised, with negative consequences for companies. After the decision has been taken to make use of cloud solutions, it is also important to continuously evaluate and monitor responses to the known risks, and to identify the potential for new ones (New Zealand Government 2009:6; Protiviti 2012:6). Because South African companies are increasingly making use of cloud computing, and in view of the fact that the POPI Act will come into effect in 2016, it is imperative that internal auditors augment their knowledge base, and enhance their skills so that they can provide the requisite levels of assurance (Cloud Security Alliance 2011:46; IIA Dallas 2012:26).

4.4.1 Data location

When cloud solutions are hosted outside national borders, it is possible that neither the primary locations nor the backup locations of the data centres to which personal information is transferred are known to the company (Protiviti 2012:2; Chivers & Kelly 2012; Chan *et al* 2012:14). Thus transferring data outside national borders can limit the control that companies can exercise over their personal information (New Zealand Government 2009:6; Chan *et al* 2012:5; European Commission 2012:5). This will in turn have a direct bearing on the security of the personal information, as it may be difficult to establish the jurisdiction in which the data is stored, which will in turn affect the ability of companies to show compliance with personal information protection requirements (Chan *et al* 2012:5, 14).

Internal auditors give assurance regarding the management of risks associated with data locations by conducting audits (including physical audits of actual locations), before the company signs contracts, service level agreements (SLAs) and operation level agreements (OLAs) with service providers (Noltes 2011: 34-36; Bortz 2012; Sammut 2013). Simultaneously, company management must be assisted to understand the information protection and data security issues, and the legislative and regulatory prerequisites which will have an impact on security, before making use of transborder clouds (Chan *et al* 2012:14). If data centres are situated in locations with inadequate or incompatible data protection laws (laws which are not comparable with the POPI Act), internal auditors can advise companies to negotiate a location change to meet regulatory requirements, or to find alternative service providers in more POPI-compliant jurisdictions, as the consequences of failing to comply with the Act are significantly dire.

4.4.2 Security

Security is a serious concern when transferring information to a transborder cloud (Krutz & Vines 2010:20; Bortz 2011b), and effective security is key to successful transfer. Security risk management includes the prevention of data leakages and loss, and the limiting of opportunities for malicious insiders and cyber-attacks (Chan *et al* 2012:5). Threats to security are of particular concern and require intensely focused attention because, by making use of cloud service providers and transferring information outside South Africa, companies are introducing the additional risks that arise when they surrender the right to respond directly to events which may affect the integrity of personal information now residing in cross-border clouds (New Zealand Government 2009: 22; Hurwitz *et al* 2009:102; Bortz 2011b).

Condition 7 of the POPI Act (s 19) states that companies must put ‘security safeguards’ in place in order to protect personal information against threats (Grant Thornton 2014). The nature of security threats is evolving at a rapid pace and these need to be assessed regularly (New Zealand Government 2009:23). New methods of attack are constantly being employed and it is imperative that internal auditors keep abreast of new threats by engaging in fora where attacks on cloud information and security issues are discussed (Fowler 2003:1; IIA 2004:171; PwC 2012:8). It is also necessary for internal audit to develop new skills and tools in order to identify data security risks and make sure that their companies implement the correct policies, processes and controls to secure personal information in the cloud (ENISA 2009:19; PwC 2012:10). To provide security assurance regarding this cloud information, internal audit needs to make it clear, usually through the audit committee, that information management and security are the joint responsibility of the board and management, and is not just an IT departmental issue (PwC 2012:10).

Companies must ensure that internal audit can regularly audit the information management security processes that are in place and provide the board with its assurance reports (IIA 2004:171; Bortz 2012). Comprehensive assessments and continuous monitoring of personnel skills, policies, procedures and controls have to be conducted to identify any weaknesses which could result in security breaches, both internally and at service provider locations (Cloud Security Alliance 2011:75-80; UK Government 2012:14; PwC 2012:8). This includes conducting vulnerability assessments and penetration tests (Hahn *et al* 2006:21; Cloud Security Alliance 2011:123, 128). It is also necessary for internal audit to have the ability to assess the service providers’ security policies and security certifications, to ensure that the level of service that is being provided meets the needs of the company (Bortz 2011b; European Commission 2012: 22; Noltes 2011:19).

4.4.3 Privacy

The protection of privacy is a risk management issue (IIA 2004:203; Hahn *et al* 2006:1). Companies must manage personal information effectively in order to maintain their good reputations. This includes ensuring that privacy laws are adhered to and that data subjects’ privacy rights are protected when personal information is collected and transferred to transborder clouds (New Zealand Government 2009:25; Krutz & Vines 2010:42, 49). According to Bortz (2011b), loss of privacy is one of the biggest risks that cloud users face. It is therefore necessary, as part of the audits that internal auditors undertake, to ensure that service providers have adequate privacy policies, protection procedures and controls in place before any contract is signed (Bortz 2011b; Hahn *et al* 2006:5). Breaches in security and privacy, which could compromise the personal information that is transferred outside South Africa to the cloud, can result in severe penalties and jail time, as is stipulated in the POPI Act, in addition to reputational damage to organisations (PwC 2012:2-5; Kafouris 2014).

Internal auditors can also give assurance by working with legal counsel to assess the degree to which the right to privacy which is given effect by the company’s policies, procedures and controls in relation to personal information, is also applicable (practically enforceable) to data that is transferred to the cloud. A clear understanding of the data management process is essential if internal auditors are going to perform regular reviews of these processes, to test their efficacy and identify any threats (Hahn *et al* 2006:4, 20; Grant Thornton 2014). Performing gap analyses of information flows and management procedures in internal procedures, and recommending implementation of best practice to assess consistency and compliance, is something that internal auditors can do to provide further assurance that privacy is being protected (Hahn *et al* 2006:5).

4.4.4 Legal compliance

There are national and regional laws and regulations which require that personal data be protected (Cloud Security Alliance 2011:36). Compliance with these laws and regulations is a crucial starting point for the protection of personal information and the right to privacy (Hahn *et al* 2006:18). Hence, when making use of cloud solutions, companies must ensure that they adhere to legal and regulatory requirements (Cloud Security Alliance 2011:38, 47; Protiviti 2012:2).

Personal information has to be managed in accordance with the requirements of the POPI Act. More specifically, for transborder transfer of data to the cloud, section 72 has to be complied with (Watson 2013; De Stadler 2013b). (Section 72 requires the cloud service provider to have in place "substantially similar" legal and/or corporate rules to those present in the POPI Act.) In order to give assurance with regard to the legal compliance risks associated with the transfer of personal information to the transborder cloud, internal auditors must have a good understanding of the POPI Act's requirements in general and of section 72 in particular. Companies should have processes in place that ensure compliance in every area of the business that handles personal information (Watson 2013; De Stadler 2013b).

Assurance can only realistically be given once an assessment of staff training and awareness programmes has been undertaken, and internal auditors are confident that there is an organisational culture of compliance (IIA 2004:180; UK Government 2012:21). An evaluation of the legal aspects of policies, procedures, processes and controls by internal audit will also assist companies to achieve their compliance goals (Bortz 2011b; Cloud Security Alliance 2011:48 UK Government 2012:22).

4.4.5 Cloud service providers

Cloud solutions are often provided by independent cloud service providers (as opposed to globally represented corporates with their own corporately managed (internal) cloud service). By contracting providers of cloud services to store/secure/manipulate/manage their data, companies thus cede to outsiders control over the personal information originally obtained by and entrusted to these companies (New Zealand Government 2009:6). Therefore, these cloud service providers have to be carefully evaluated, and selected and managed in a manner that ensures that the solutions they provide will benefit the company, and will not expose it to undue risks that may negatively affect the business (Bortz 2011b; Protiviti 2012:3). Ultimately, the company is responsible for the security of the personal information, even if it engages cloud service providers and gives them physical/electronic control over the information. As there may be jurisdictional issues associated with engaging service providers whose services are domiciled and/or provided from outside South Africa, specialist legal advice should be obtained when agreements are drafted and before they are signed (New Zealand Government 2009:28)

In providing assurance, the internal auditor's role includes investigating all service providers before services are procured, and thereafter constantly monitoring them to ensure that the required services are being provided in a manner that demonstrates compliance with legislative requirements (UK Government 2012:12; Protiviti 2012:6). A "right-to-audit" clause must be included in all agreements between companies and cloud service providers (Cloud Security Alliance 2011:50; Chan *et al* 2012:13; Bortz 2012; Teremi 2012:13). Internal auditors must also participate in the negotiation or review of all service provider contracts and SLAs to ensure that they are comprehensive; contracts must provide information about the services to be provided, the location of data centres to which personal information will be transferred, the processes and procedures involved in managing personal information in the cloud, and finally, the penalties for breaches must be explicit and comprehensive (Noltes 2011:24; Protiviti 2012:5; Chan *et al* 2012:13; Bortz 2012). Internal auditors must review these service provider contracts, agreements and processes to ensure that all the requirements of section 72 of the POPI Act are met, because liability for any compliance failures rests with the company.

5 CONCLUSIONS AND FURTHER RESEARCH

As transborder data flows increase globally, there is a need to regulate the management of information when it is transferred outside its country of origin (Kuner 2013:1). It is therefore important for companies to measure the risks that are present when transferring personal information outside South Africa (even though this is permissible in terms of section 72 of the POPI Act), and then decide whether it is prudent to do so. It is clear from the case of the Zurich Insurance data leak that there can be serious financial and reputational consequences to any kind of breach or failure in the measures employed to protect personal information (Telavance 2012; Ernest & Young 2011:5-6; PwC 2012:7-8; Chan *et al* 2012: 4-6, 17-20; CIIA UK 2014:1-2).

In South Africa, the regulation of personal information transfer to transborder clouds is an exciting new area where the issues of compliance with the POPI Act (legal), cloud computing (IT) and internal auditing (auditing and risk management) intersect, and presents opportunities for the internal auditing profession to play a pioneering and critical role in enabling the successful integration of these diverse fields. The importance of having a skilled and active internal audit function has been repeatedly emphasised: the diversity of their skillset enables them to play a leading role in this new area. This research has attempted to show that internal auditors, as independent assurance providers with a keen understanding of their companies' business strategies, operations and goals, can lead their companies to the achievement of compliance with the POPI Act, by helping organisations to successfully mitigate the risks that flow from the use of transborder clouds for storage and processing of personal information.

Internal auditors can play a crucial role in cloud computing risk management in that they are able to give assurance on the management of the five emerging risks associated with the transfer of personal information to the transborder cloud, risks associated with data location, security, privacy, legal compliance and cloud service providers' operational procedures. Knowledge of these risks is critical in order for internal auditors to audit transborder cloud computing solutions effectively and thus to add value to their organisations (Nicolaou *et al* 2012). The auditing of cloud service providers (to assess the solutions they provide and the adequacy of these to meet the company's needs), is a key internal audit function (Bortz 2011b; Protiviti 2012:3). If the wrong service providers are engaged, it may result in the risks being realised, and the personal information in the transborder cloud being lost or compromised. Internal audit can provide assurance on risks associated with data location and security by conducting audits (including physical audits of actual locations and certifications), before the signing of agreements with service providers, as well as by determining the legal and regulatory regimes that pertain at the locations of transborder cloud data centres, and the adequacy of security measures they have in place to protect personal information (Cloud Security Alliance 2011:75-80; Noltes 2011:34-36; Bortz 2012; Sammut 2013). An internal audit assessment of the company's culture of compliance (including general awareness and staff training programmes, policies and controls), can provide assurance that the protection protocols for personal information are congruent with the requirements of the POPI Act (IIA 2004:180; UK Government 2012:21). Internal audit can also give assurance that the right to privacy is being protected by reviewing company and service provider privacy policies and procedures. In addition, gap analyses may be performed to ensure that all weaknesses are being identified and mitigated (Hahn *et al* 2006:5; Grant Thornton 2014).

As this is a new area, this research is necessarily introductory and is intended to give some insight into the impact that the POPI Act has already had on the specific area of transborder transfers of personal information. Further research can and must be undertaken on the development of comprehensive organisational frameworks and audit plans for this area of business life. At a national level, regulations should be developed (as has been done overseas), where data protection laws have led to research on and the publication of guidelines for cloud computing, with a focus on data protection. South Africa has developed data protection legislation based on international standards, and this work can be taken further by the development of comprehensive regulations regarding management of personal information in specific areas such as cloud computing.

Acknowledgement

Thanks to Tammy Bortz, Director at Werksmans Attorneys, for providing initial insights into cloud computing and POPI.
Thanks to Theodore Watson, Attorney at Microsoft South Africa, for kindly sharing his knowledge, practical experience and time for this research.

REFERENCES

AbuOliem, A. 2013. Cloud computing regulation: An attempt to protect personal data transmission to cross-border cloud storage services. *International Journal of Computer and Communication Engineering*, 2(4):521-525.

AON South Africa. 2012. *South African businesses unprepared for the growing risk of cyber attacks.* [Online]. https://www.aon.co.za/index.php/en/news-articles/244-south-african-businesses-unprepared-for-the-growing-risk-of-cyber-attacks (Accessed: 28 April 2014).

Barac, K. & Coetzee, G.P. 2012. The effect of specific internal audit function features on the demand for internal auditors in South Africa. *The Southern African Journal of Accountability and Auditing Research*, 13:36.

BBC News. 2010. *Zurich Insurance fined £2.3m over customers' data loss.* [Online]. http://www.bbc.co.uk/news/business-11070217 (Accessed: 28 April 2014).

Bilton, A. 2011. Internal audit and the cloud: part 1. *Audit & Risk.* [Online]. http://auditandrisk.org.uk/features/internal-audit-and-the-cloud-part-1 (Accessed 2 May 2014).

Bortz, T. 2011a. (t.bortz@werkemans.co.za) Discussion on cloud computing. [Email to:] Jangara, T.C. (tjangara@deloitte.co.za). January 2011.

Bortz, T. 2011b. *South Africa: SA business warned to mitigate cloud computing risks*. Werksmans Attorneys. [Online]. http://www.werksmans.com/virt_media/sa-business-warned-to-mitigate-cloud-computing-risks/ (Accessed: 9 January 2012).

Bortz, T. 2012. Contracting in the cloud (Part 2) – so what's new? *Legal Brief Werksmans Attorneys*. [Online]. http://www.werksmans.com/legal-briefs-view/contracting-in-the-cloud-part-2-so-whats-new/ (Accessed: 24 November 2013).

CBS News. 2013. *Sony fined in U.K. over PlayStation cyberattack*. [Online]. http://www.cbsnews.com/news/sony-fined-in-uk-over-playstation-cyberattack/ (Accessed: 28 April 2014).

Chan, C., Leung, E. & Pili, H. 2012. *COSO Enterprise risk management for cloud computing*. Crowe Horwarth LLP. [Online]. http://www.coso.org/documents/Cloud%20Computing%20Thought%20Paper.pdf (Accessed: 20 January 2014).

Chartered Institute for Internal Auditors United Kingdon (CIIA UK). 2014. What is internal audit? [Online]. http://www.iia.org.uk/about-us/what-is-internal-audit/ (Accessed: 27 June 2014).

Chivers, D. & Kelly, T. 2012. Why SA companies should take heed of the Protection of Personal Information Bill. *Deloitte SA Blog*. [Online]. http://deloitteblog.co.za/tag/protection-of-personal-information-bill/ (Accessed: 27 February 2014).

Chung, M. & Hermans, J. 2010. *KPMG's 2010 Cloud Computing Survey*. Netherlands. KPMG.

Cloud Security Alliance. 2011. *Security Guidance for Critical Areas of Focus in Cloud Computing v3.0*. [Online]. https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf (Accessed: 15 January 2014).

De Stadler, E. 2013a. *Intro to the Protection of Personal Information bill (part 1): When does PoPI apply?* [Online]. http://www.esselaar.co.za/legal-articles/intro-protection-personal-information-bill-part-1-when-does-popi-apply (Accessed: 4 February 2014).

De Stadler, E. 2013b. *Intro to POPI (part 8): Trans-border information flow*. [Online]. http://www.novcon.co.za/articles/intro-popi-part-8-trans-border-information-flow (Accessed: 4 February 2014).

Dhont, J. & Woodcock K. 2014. *South Africa enacts new data protection law.* Lorenz International Lawyers. [Online] http://www.lorenz-law.com/wp-content/uploads/South-Africa-Enacts-New-Data-Protection-Law.pdf (Accessed: 14 February 2014).

Dlamini, A. 2013. POPI headache looms. *IT News Africa* October 14, 2013. [Online]. http://www.itnewsafrica.com/2013/10/popi-headache-looms/ (Accessed: 5 January 2014).

European Network and Information Security Agency (ENISA). 2009. *Cloud computing: Benefits, risks and recommendations for information security*. [Online]. https://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment (Accessed: 23 July 2014).

Ernest & Young. 2011. *Internal audit's evolving role: A proactive catalyst of business improvement.* [Online]. http://www.tapestrynetworks.com/upload/Tapestry_EY_ACLN_InSights_Apr11.pdf (Accessed 28 June 2014).

European Commission. 2012. Article 29 Data Working Party. *Opinion 05/2012 on Cloud Computing.* [Online]. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf (Accessed: 14 February 2014).

European Parliament and Council. 1995. EU Data Protection Directive (Directive 95/46/EC) (EU Directive). [Online]. http://www.dataprotection.ie/docs/EU-Directive-95-46-EC-Chapter-1/92.htm (Accessed 14 February 2014).

Fick, J. 2010. Directorship: A king's ransom. *IOD Directorship Magazine*. Jan - Mar 2010, 22-25.

Fischer, P. 2012. Global standards: Recent developments between the poles of privacy and cloud computing. *3 JIPITEC 1* para 33-8.

Fowler, S. 2003. *Information classification: Who, why and how*. SANS Institute.

Gardner, Z. 2012. Protection of Personal Information Bill, No. 2. *ENS Africa*. [Online]. http://www.ensafrica.com/news/Protection-of-Personal-Information-Bill-No-2?Id=816&STitle=corporate+commercial+ENSight (Accessed: 3 February 2014).

Gartner, 2010. *Gartner says worldwide cloud services market to surpass $68 billion in 2010*. [Online]. http://www.gartner.com/newsroom/id/1389313 (Accessed: 22 July 2014).

Grant Thornton. 2014. New POPI Act brings operational, financial and legal burden to businesses and their third party outsource service providers – Grant Thornton. [Online]. http://www.gt.co.za/news/2014/05/new-popi-act-brings-operational-financial-and-legal-burden-to-businesses-and-their-third-party-outsource-service-providers-grant-thornton/ (Accessed: 19 June 2014).

Hahn, U., Askelson, K. & Stiles, R. 2006. Global Technology Audit Guide 5: Managing and auditing privacy risks. *The Institute of Internal Auditors (IIA)* 1-25.

Hon, W.K., Hornle, J. & Millard C. 2011. *Data protection jurisdiction and cloud computing: When are cloud users and providers subject to EU data protection laws?* The cloud of unknowing, Part 3. Legal Studies Research Paper no 84/2011. Queen Mary University of London, School of Law.

Hsu, W-H.L. 2012. Conceptual framework of Cloud Computing Governance Model: An education perspective. *IEEE Technology and Engineering Education (ITEE)*, 7(2) June 12-16.

Hurwitz, J., Bloor. R., Kaufman, M. & Halper, F. 2009. *Cloud computing for dummies.* Indiana: Wiley.

Institute for Directors (IOD). 2009. *King Report on Corporate Governance in South Africa*. IOD: South Africa.

Institute for Internal Auditors Research Foundation (IIA). 2004. *The Professional Practices Framework for Internal Auditing (PPF).* [Online]. http://www.iadb.org/aug/includes/ProfPracFramework.pdf (Accessed: 28 July 2014).

Institute for Internal Auditors Dallas Chapter (IIA Dallas). 2012. *Cloud computing: A study of internal audit's preparedness in the Dallas area.* Institute of Internal Auditors. [Online]. https://na.theiia.org/iiarf/Public%20Documents/IIA%20Dallas%20Research%20Project%20-%20Final%20Submission.pdf (Accessed: 26 June 2014).

IT Governance Network. 2010. *Privacy & protection of personal information*. [Online]. http://deloitteblog.co.za/2014/01/16/cloud-computing-and-ppi-finding-your-bearing/ (Accessed: 28 June 2014).

Kafouris, D. 2011. Deloitte talks about maintaining privacy and security in the cloud. *Deloitte SA Blog*. [Online]. http://deloitteblog.co.za/tag/protection-of-personal-information-bill/ (Accessed: 27 February 2014).

Kafouris, D. 2014. Cloud computing and PPI: Finding your bearing. *Deloitte SA Blog*. [Online]. http://deloitteblog.co.za/2014/01/16/cloud-computing-and-ppi-finding-your-bearing/ (Accessed: 27 February 2014).

Kolver, L. 2014. SA businesses not ready for POPI implementation – Grant Thornton. Polity.org.za. [Online]. http://www.polity.org.za/article/sa-businesses-not-ready-for-popi-implementation-grant-thorton-2014-03-06 (Accessed: 06 June 2014).

KPMG, 2008. *The evolving role of the internal auditor: Value creation and preservation from an internal audit perspective.* [Online] https://www.kpmg.com/ZA/en/IssuesAndInsights/ArticlesPublications/Risk-Compliance/Documents/The%20Evolving%20role%20of%20the%20Internal%20Auditor.pdf (Accessed 19 June 2014).

Krutz, R.L. & Vines, R.D. 2010. *Cloud security: A comprehensive guide to secure cloud computing.* United Kingdom: John Wiley & Sons.

Kuner, C. 2011. *Regulation of transborder data flows under data protection and privacy law: Past, present and future*. OECD Digital Economy Papers, No. 187, OECD Publishing.

Kuner, C. 2013. *Transborder data flows and data privacy law*. United Kingdom: Oxford University Press.

Lamprecht, I. 2013. *Few organisations ready for Popi.* Moneyweb. [Online]. http://www.moneyweb.co.za/moneyweb-corporate-governance/few-organisations-ready-for-popi (Accessed: 24 February 2014).

Liston, S. 2012. *The cloud: Data protection and privacy whose cloud is it anyway?* GSR Discussion Paper. [Online]. http://www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR12/documents/GSR12_Privacy_Liston_6.pdf (Accessed: 24 February 2014).

Marks, N. 2010. *The future of the internal audit profession.* [Online]. http://normanmarks.wordpress.com/2010/06/29/the-future-of-the-internal-audit-profession/ (Accessed: 29 July 2014).

New Zealand Government. 2009. *Government use of offshore information and communication technologies (ICT) service providers: Advice on Risk Management.* New Zealand. [Online] http://ict.govt.nz/assets/Uploads/Drupal/offshore-ICT-service-providers-april-2007.pdf (Accessed: 10 March 2014).

Nicolaou, C.A., Nicolaou, A.I., & Nicolaou, G.D. 2012. Auditing in the cloud: Challenges and opportunities. *The CPA Journal.* New York State Society of Certified Public Accountants. [Online]. http://callcenterinfo.tmcnet.com/news/2012/02/27/6147821.htm (Accessed 28 June 2014).

Noltes, J. 2011. Data location compliance in cloud computing. Masters thesis, University of Twente. [Online]. http://essay.utwente.nl/610421 (Accessed 01 July 2014).

O'Donoghue, C. 2013. New data protection law for South Africa. *Mondaq*. [Online]. http://www.mondaq.com/x/283662/data+protection/New+Data+Protection+Law+For+South+Africa (Accessed: 20 January 2014).

Phakathi, B. 2014. Business 'not ready' for personal information law. *Business Day.* [Online]. http://www.bdlive.co.za/business/2014/03/07/business-not-ready-for-personal-information-law (Accessed: 15 March 2014).

Pieters, M. 2013. Is cross border data transfer prohibited in terms of POPI?' *Bandwidth Blog* 22 January 2013. [Online]. http://www.bandwidthblog.com/2013/01/22/is-cross-border-data-transfer-prohibited-in-terms-of-popi/ (Accessed: 14 January 2014).

Protiviti. 2012. *Internal Audit's Role in Cloud Computing.* [Online]. http://www.protiviti.com/en-US/Documents/White-Papers/Risk-Solutions/IA-Role-Cloud-Computing-Protiviti.pdf (Accessed 23 April 2014).

PwC. 2011. *Cloud computing and the internal audit function*. [Online]. http://www.pwc.com/us/en/issues/cloud-computing/navigating-the-risks-of-cloud-computing.jhtml (Accessed: 23 June 2014).

PwC. 2012. *Fortifying your defences: The role of internal audit in assuring data security and privacy.* [Online]. http://www.pwc.com/en_US/us/risk-assurance-services/assets/pwc-internal-audit-assuring-data-security-privacy.pdf (Accessed: 23 June 2014)

Sammut, G. 2013. Internal audit takes on emerging technologies. *Mondaq*. [Online]. http://www.mondaq.com/x/216430/technology/Internal+Audit+Takes+On+Emerging+Technologies (Accessed: 28 June 2014).

Senathipathi, K., Chitra, S., Angeline Rubella, J. & Suganya, M. 2013. A cross border access to data stored in the cloud. *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)* 2(10):2707–2714.

Slater, W. 2012. The roles of the internal audit team in cloud computing. *Bellevue University.* [Online]. http://www.billslater.com/writing/CYBR_615_Week_01_Written_Homework_Assignment_from_W_F_Slater_.pdf (Accessed: 23 June 2014).

South African Government. 2013. *Protection of Personal Information Act* 4 of 2013. Pretoria: Government Printer.

Speckman, A. 2014. African rivals pass SA in cloud computing. *Business Report*. [Online]. http://www.iol.co.za/business/companies/african-rivals-pass-sa-in-cloud-computing-1.1669604#.U3k4esuKBjp (Accessed 2 April 2014).

Telavance. 2012. Risk management: How internal audit can play a key role. [Online] http://www.telavance.com/advantage/previous-issues/current-issue/risk-management-how-internal-audit-can-play-a-key-role/ (Accessed 28 June 2014).

Teremi, I. 2012. Privacy, data flows and the cloud. *Practical Advice_ Commercial Outcomes. Kreisson Legal*. [Online]. http://www.kreissonlegal.com.au/wp-content/uploads/2012/08/2-Privacy-Data-Flows-Cloud.pdf (Accessed: 5 March 2014).

The Institute of Chartered Accountants in England and Wales (ICAEW). 2004. *Guidance for audit committees: The Internal Audit function.* The Institute of Chartered Accountants in England and Wales.

The Institute of Internal Auditors. 2013. *International Standards for the Professional Practice of Internal Auditing.* [Online]. http://www.theiia.org/guidance/standards-and-guidance/ippf/standards/full-standards/?search=risk (Accessed: 7 April 2015).

Tomaszewski, J. 2013. A board's legal obligations for the cloud: You have to carry an umbrella. *Business Law Today*. [Online]. http://www.americanbar.org/publications/blt/2013/08/03_tomaszewski.html Accessed: 20 January 2014.

United Kingdom (UK) Government. 1998. Data Protection Act. Information Commissioner's Office (ICO), 2012. *Guidance on the use of cloud computing*. United Kingdom. [Online]. http://ico.org.uk/for_organisations/guidance_index/~/media/documents/library/Data_Protection/Practical_application/cloud_computing_guidance_for_organisations.ashx (Accessed: 5 March 2014).

Von Solms, R. & Viljoen, M. 2012. Cloud computing service value: a message to the board. *South African Journal of Business Management* 43 (4):73-81.

Watson, T. 2013. Data sovereignty under the protection of personal information act. *Microsoft Press Article.* [Online]. http://www.microsoft.com/southafrica/press/Pages/Article.aspx?id=44. (Accessed: 10 February 2014).

Watson, T. 2014. Discussion at Microsoft South Africa. Bryanston. February 2014.

Walker, D. & Meiring, I. 2010. *King Code and developments in corporate governance.* Werksmans Attorneys.

Wehler, A. 2013. South African Parliament passes the Protection of Personal Information Bill. *The Chertoff Group*. [Online]. http://safegov.org/2013/9/16/south-african-parliament-passes-the-protection-of-personal-information-bill (Accessed: 10 February 2014).

Wolfe, H.B. 2011. Cloud computing: The emperor's new clothes of IT. *Proceedings of Informing Science & IT Education Conference (InSite)*. [Online]. http://proceedings.informingscience.org/InSITE2011/InSITE11p599-608Wolfe281.pdf (Accessed: 9 January 2012).

Internal audit's role in embedding governance, risk, and compliance in state-owned companies

T M Chikwiri
Department of Auditing
University of Pretoria

S P de la Rosa
Murray and Robberts

ABSTRACT

The increase in the number of company failures, and in the occurrence of corporate fines and lawsuits due to noncompliance with statutes and regulations, has been attributed to inadequate or failed governance, risk, and compliance (GRC) processes. The purpose of this study is to explore internal audit's role in embedding GRC processes in state-owned companies. Internal auditors were found to be actively involved in assisting their organisations in embedding GRC processes, and in improving their GRC maturity through spearheading and coordinating the implementation of combined assurance protocols. In this regard internal auditors were found to be most effective when they have buy-in from top management.

Key words

Chief audit executives (CAES); embedding; governance; risk and compliance (GRC); GRC maturity; internal audit function; role; state owned companies (SOC)

1 INTRODUCTION

In a research study conducted on chief audit executives' (CAEs) strategic relationships, one chief financial officer (CFO) was quoted as saying, "… internal audit findings are worthless, the internal audit function should focus on improving the control environment as they know best practices and they should share these and be proactive" (Abdolmohammadi, Ramamoorti & Sarens 2013:35). In light of this statement, this study examines the role of internal audit in embedding governance, risk, and compliance (GRC) protocols in South African state-owned companies (SOCs). Despite the sentiment expressed in the above quote, international research has more recently shown that management is interested in internal auditors that spend their time providing insight, advice and assistance on embedding GRC processes in their organisations (Chambers 2014:57).

The current state of GRC processes in organisations is still described as "fragmented", "not unified" and "disorganised", suggesting that the implementation of GRC processes still needs to evolve (Hoon 2011:22; Anderson 2011:60). The gap between recent literature (theory) and current practice is magnified by the fact that most organisations still see governance, risk, and compliance as three cost centres, rather than as a unitary investment (Boultwood 2013; Steffee 2012: 12). GRC professionals are thus faced with the challenge of justifying the investment value of the concepts of governance, risk, and compliance to the board and executive management (Raths 2011: 18). Fragmented GRC processes also hinder the implementation of internal audit strategies.

Furthermore, the business case for embedding GRC in organisational structures as a triune (a singular concept arising from the integration of three distinct business functions), is based on the premise that these individual functions are conventionally managed by different people in relative isolation, each in pursuit of their own individual performance targets (Pickett 2011:233). Raths (2011:19) points out that in most organisations surveyed there is no single person with total responsibility for GRC activities. This encourages a silo approach to these activities, resulting in a persistent disconnection between individual GRC functions (Meiselman 2007:40; Anand 2010:57). This in turn results in duplication of efforts and associated inefficiencies, inconsistencies, and a lack of transparency and uniformity in the performance of these functions (Frigo & Anderson 2009b:34; Raths 2011:19).

The problem of inconsistent GRC across organisations (Stanford 2004:45) has resulted in an increase in incidents of corporate fines, judicial sanctions and lawsuits, and downgrades in credit ratings (Balachandran & Sundar 2013:41; Greengard 2011:24; Anon 2011:39). This may be attributed to weak, ineffective and/or failed GRC processes (Frigo & Anderson 2009b:34). Internal auditors face strong pressures from stakeholders to improve GRC within organisations. This has been complicated by aspects such as lack of clarity, or uncertainty, about internal audit's role in embedding GRC processes, and ongoing difficulty in narrowing the stakeholder expectation gap. Balachandran & Sundar (2013:41) emphasise that the consequences of inadequate GRC are severe and can lead to insolvency – hence the necessary incongruity of increased spending on GRC functionality in a period of tightening budgets.

Within the South African context, PriceWaterhouse-Coopers' 2011 study (PwC 2011:5) identified inadequate governance frameworks as one of the primary causes of poor performance by SOCs. The challenges associated with implementing suitable governance frameworks have increased the demand for auditors with GRC competencies, as boards raise concerns about the design and management of such systems (Konstans, Radhakrishnan, Switzer, & Williams 2011:55; McGraw 2012:18). Furthermore, boards are concerned that the fragmented view of risks and associated issues arises because GRC activities are sub-optimally integrated (Raths 2011:18; Anand 2010:57; Konstans *et a*l 2011:56). In addition, the current wave of regulatory changes and reforms, and the onerous compliance requirements coupled with increasingly stringent budgetary constraints, has contributed to the expansion of GRC functions (Konstans *et al* 2011:55; Raths 2011:19). The future belongs to well-governed, compliant, and risk-intelligent organisations (Metricstream 2013), and internal auditors have a part to play in building such organisations, through an active role in embedding GRC processes.

The empirical evidence provided by this study will benefit those CAEs who are actively engaged in embedding GRC functions in their organisations. In addition, professional and public sector bodies within South Africa should also benefit by using the findings of this study to strengthen the supporting role of their internal audit functions.

This study is organized as follows: section 2 identifies the research objectives, scope, methodology, and limitations of the research methods. Section 3 contains an examination of current literature on GRC, followed by analysis and discussion of the interview results. The final section (section 4) summarises the contribution of the study to the internal audit profession's expanding business role, and suggests the next steps to be taken in the roll-out of GRC within SOCs.

2 RESEARCH OBJECTIVES, SCOPE, METHODOLOGY, AND LIMITATIONS

The aims of this study are as follows: firstly, to examine the concepts of GRC and maturity models and how GRC processes are embedded. Secondly, the study seeks to better understand the state of GRC processes and practices within SOCs, particularly internal audit's role in embedding these processes and achieving effective integration. Thirdly, the study seeks to understand how the GRC's present maturity stage within a SOC affects the role that internal audit should play in embedding such processes, while pursuing the intention of improving the maturity level. Lastly, the study records the challenges faced and lessons learnt by internal auditors while participating in the process of embedding GRC principles in the SOC.

Research approach

A qualitative approach was considered to be appropriate for this study, as it allows for deeper understanding of the subject matter (Creswell & Clark 2007:8; Verschuren & Doorewaard, 2010:78; Teddie & Yu 2007:77; Bloomberg & Volpe 2012:9; Yin 2009:23). Qualitative research rests on an interpretive or social constructivist basis: the distinction lies between objective and subjective knowledge (Verschuren & Doorewaard 2010:78; Bloomberg & Volpe 2012:29). This study has been based on an interpretivist approach, as reliance has been placed upon the participants' views (perceptions and/or interpretations) of the situation being studied (Creswell & Clark 2007:8; Verschuren & Doorewaard 2010:78; Bloomberg & Volpe 2012:30).

Data collection

In order to obtain information directly related to the process of embedding GRC, interviews were conducted with CAEs and GRC representatives at selected SOCs. The SOCs invited to participate in the research were drawn from the list of contenders for Ernst & Young's (EY) Excellence in Integrated Reporting Awards 2013. The Excellence in Integrated Reporting Awards was considered as a suitable basis for sample selection, as it allows comparison of how SOCs are complying with King III requirements through disclosure in integrated reports. Through integrated reports, SOCs have demonstrated their intent to implement King III, which enabled the comparison of how GRC is embedded in these organisations.

To secure active participation, interviewees were given assurance that their responses would not be specifically identifiable, and that they would be referred to only by their job titles in the study. In addition, the anonymity of their organisations would be maintained: it would not be possible for their specific responses and/or their organisations to be linked or identified. The sources of data for this study came from the review of documents (including annual reports and integrated reports), and from transcripts of open-ended interviews conducted by the researcher (Yin 2009:83). Insights drawn from these interviews, literature, annual reports, and associated documents were incorporated into efforts to understand the South African experience discussed in this study. With the permission of each interviewee, the face-to-face interviews were recorded digitally to enable later data analysis. The focus of the interviews was to access the insights and understanding of those involved in directing the GRC implementation processes and the operational practices in the SOCs, drawn from their hands-on experiences. Guide questions based on the literature review were developed for the interviews, and additional issues that emerged during the interview were explored immediately, and late revaluated as part of the data analysis process. Where questions did not relate to the interviewees' specific day-to-day work, their thoughts and views of such other GRC functions were asked. Interviews were conducted during the second and third quarters of 2014.

Research method

To achieve the aims of the research, a case study method was used in order to answer the "how" and "why" research questions posed by the research topic (Yin 2009:6). Yin describes case study research as "... an empirical inquiry that investigates a contemporary phenomenon in depth and within its real-life context, especially when the boundaries between phenomenon and context are not clearly evident" (Yin 2009:13). This method appeared most appropriate for this study as, according to Verschuren and Doorewaard (2010:178) and Bloomberg and Volpe (2012:43), the case study method's focus is on gathering qualitative data by generating in-depth and intensive data on a small strategic sample. This study was conducted on three of the twenty-one major SOCs and public entities in South Africa. Multiple entities (SOCs) were selected to enable replication of findings, as similarities and differences within and between SOCs were explored (Yin 2009:47). The emphasis was on comparing and interpreting the results gathered from the in-depth interviews (Verschuren & Doorewaard 2010:179). The questions were open-ended to maximise the amount and accuracy of the data offered by the interviewees (Yin 2009:9; Verschuren & Doorewaard 2010:179). The research questions were derived from and inspired by a review of current literature on GRC, and augmented by insights gained through the study of official publications, including annual reports issued by the SOCs.

Population and sample size

Most studies on GRC have been conducted within the context of heavily-regulated industries and developed countries with significantly mature consumer and financial service cultures. For example, financial institutions are generally in the lead in the implementation of broadly defined GRC requirements. The decision was therefore taken to investigate the status of GRC integration in less well-regulated and frequently ignored entities such as SOCs.

The population for this study was the 21 state owned (public) entities in South Africa, from which a sample of three was selected. These SOCs operate in different economic sectors and report to different national government departments. The SOCs were selected for this study according to three criteria: their importance and contribution to the economy; the challenges they are currently facing, and the degree to which GRC functions have been embedded in their operations, which is in turn a measure of the implementation of King III as disclosed in their integrated reports.

A number of constraints (including unavailability of potential interviewees, and time) made it impossible to engage all 21 of the SOCs. A strategic sampling method was therefore used to select SOCs with different or contrasting characteristics (Verschuren & Doorewaard 2010:1809). According to Yin (2009:13), limiting the number of participating organisations enables the comparison of data to produce more strikingly similar or contrasting results. In addition, convenience sampling was used, that resulted in the final selection of a representative sample of three SOCs for in-depth study. Convenience sampling involves identifying participants that are willing, able, and accessible (to the researcher, amongst others) as an "intermediate universe" from which the study's final participants are drawn (Teddie & Yu 2007:78).

According to the EY's Excellence in Integrated Reporting Awards 2013, the top 10 state owned entities were ranked as either "excellent", "good," "average", or "needs progress," in terms of their level of integrated reporting. The top 10 SOCs in 2013 included: Eskom; Transnet; Industrial Development Corporation of SA, Ltd; Development Bank of SA ;the South African Post Office; Airports Company of South Africa; Central Energy Fund; South African Airways; Landbank; and Trans-Caledon Tunnel Authority. To ensure that the study was objective, and to facilitate generalisations, the sample included three SOCs selected from the four ranking categories, as per the EY's Excellence in Integrated Reporting Awards 2013. The three SOCs selected will be referred to as SOC A, B, and C. The interviewees include three CAEs and three employees with GRC management responsibilities, from selected SOCs. This breakdown enabled the comparison of different viewpoints within and between organisations, and the formulation of an overview of the situation in SOCs in South Africa.

Data analysis

Failure to properly define strategies and techniques makes analysis of data difficult (Yin 2009:109). This risk was addressed by coding the recorded interviews, and then analysing and categorising the data using the ATLAS.ti qualitative analysis tool. Thereafter, the emerging common GRC themes were identified, documented, organised, and classified. According to Yin, the purpose of this software is to develop meaning and understanding from the word usage and frequency patterns found in the information gathered (Yin 2009:111). This was intended to enable the creation of convincing analytic conclusions on the implementation of GRC processes in SOCs, and on the role of the internal audit function.

Because the study examined three SOCs, cross-case synthesis was chosen as the appropriate analytical technique for the data collected. This technique enables valid conclusions to be reached as it allows the comparison of findings across SOCs (Yin 2009:15). The views of the interviewees from each GRC function were compared and an outline of their understanding of GRC was established. Conclusions as to the level of understanding of GRC processes shown by each role player interviewed were used to construct generalisations regarding the status of GRC within SOCs in South Africa.

Study limitations

This study aimed to understand, explore and explain the role of internal audit in the process of embedding GRC in SOCs. This study investigated the perceptions of CAEs and managers of GRC practices in their organisations, and of the role played by internal audit in the process. The first limitation of this study is inherent in the choice of research methodology, involving as it did the use of personal interviews, as the perceptions of interviewees on GRC may differ from practice. In addition, the sample was limited to only three SOCs out of a possible 21 major public entities in South Africa. Thus, it may not reflect the views of all CAEs in the South African SOCs environment, nor those of private sector CAEs, both in South Africa and in other countries. However, it is probable that the outcomes would be similar if the study were conducted in the private sector as, according to commentary in the EY's Excellence in Integrated Reporting Awards 2013, SOCs and private sector entities alike are embracing the 'King Code of Governance Principles'. The second limitation is that the findings of this study are specific to the South African state owned company environment. The third limitation is that the SOCs selected for this study were drawn from the rankings produced for EY's Excellence in Integrated Reporting Awards 2013, and the methodology and processes used to rate SOCs for that purpose was not reviewed.

3 LITERATURE REVIEW

Before embarking on an exploration of internal audit's role in embedding GRC within SOCs, it is necessary to outline the concepts within governance, risk, and compliance – GRC – and to provide a well-supported definition. Secondly, it is essential to understand the structures and purposes of SOCs within the context of South Africa's public sector, and to determine the state of GRC efforts within SOCs. Thirdly, the GRC maturity model will be examined, as will the concepts used to establish how to achieve maximum benefit for SOCs by embedding GRC processes in their operational frameworks. Lastly, based on the current state of GRC in SOCs and the SOCs' levels of GRC maturity, an understanding of the role that the internal audit function should play in embedding GRC will be explored.

3.1 The GRC concept

GRC is a catch-all acronym that has a variety of meanings and interpretations. According to Steinberg (2010:40), GRC is a combination of interrelated concepts which include governance, risk, and compliance (Open Compliance and Ethics Group's definition, as quoted by Marks 2010:25; Frigo & Anderson 2009b:35). The focus of GRC is on building a unified relationship between these elements, to increase their individual effectiveness (KPMG 2012). The common elements of GRC are compliance with statutes, laws and regulations specific to the business, risk assessments and reduction of risk exposure, and the effective implementation of business processes and policies (Anderson 2011:60). There is however ongoing debate on the meaning of the 'C' in GRC, with some authors referring to it as 'controls,' and others, 'compliance' (The Institute of Internal Auditors Research Foundation (IIARF) 2013:20). In this research paper, the 'C' in GRC means 'compliance'. Some of the more lucid definitions of the components of GRC are quoted below.

Governance is:

- "...the combination of processes and structures implemented by the board to inform, direct, manage, and monitor the activities of the organization toward the achievement of its objectives" (IIA 2013).
- "...the arrangements put in place to ensure that the intended outcomes for stakeholders are defined and achieved" (International Federation of Accountants 2014:5).
- "...the way organisations are directed and controlled" (Cadbury 1992; Pickett 2011:13).
- "...the ethical direction and control of an organisation to achieve its objectives while considering stakeholders needs and expectations" (IODSA 2009; Naidoo 2009:15).
- "...a set of relationships between a company's management, its board, its shareholders and other stakeholders and structures through which company objectives are set, attained and monitored" (OECD 2004:11).

For the purpose of this study, **governance** will be defined as "the set of processes that encompass the interaction of the board and management as they strategically direct and control the organisation to achieve its objectives".

Risk management is a key driver for GRC (Pickett 2011:82; Lamont 2012:8; Greengard 2011:24) and is variously defined as:

- "...the process of addressing organisational risks across the activities of the organisation to achieve sustained benefit" (Institute of Risk Management UK 2002:2).
- "...a process, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives" (COSO 2004).
- "...the coordination of activities in respect of managing organisational risk" (ISO 31000 2009).
- *"...the process of identifying, assessing, managing*, and controlling actual or possible events or conditions to ensure that the organisation achieves its objectives'' (IIA 2013; Pickett 2011:44).
- "...a systematic and formalised process to identify, assess, manage and monitor risks" (National Treasury of South Africa 2010).
- "...an organised process of identifying, assessing and managing risks at strategic and or operational level" (Coetzee 2010:155).

For the purposes of this study, **risk management** will be defined as the *"identification, evaluation and management of events that could positively or negatively affect the achievement of an organisation's objectives"*.

Compliance is defined as the adherence to policies, procedures, laws, codes, standards and regulations that govern the business (IIA 2013; Mitchell & Switzer 2009:10; IODSA 2009:89). Compliance should also consider both the rights and the obligations of the organisation (IODSA 2009:89). For this study, **compliance** is defined as "*the process of adhering to internal and external requirements, such as policies,* *and regulatory mandates and standards that govern the organisation*".

As The Institute of Internal Auditors Research Foundation (IIARF) (2013:20) states, there is as yet no universally recognised definition of "GRC". It is variously defined as follows in the literature:

- "...the amalgamation and collaboration of roles and processes for risk and control functions" (The RMIA 2012:7).
- "…a strategic approach to integrating risk management, regulatory compliance, controls, assurance structures and processes, and intelligently using IT data management structures supported by a strong organisational culture" (KPMG 2012).
- "…the way in which the board ensures an organisation attempts to meet its objectives by identifying and managing risks and obtaining assurance that controls (including compliance) are in place and efficiently and effectively mitigating risk" (IIARF 2013).
- "…a capability to reliably achieve objectives [governance] while addressing uncertainty [risk management] and acting with integrity [compliance]" (Mitchell and Switzer 2009:9).

Taking into account the broad scope of the above definitions, **GRC** will be defined as *"the integration of processes that encompass the interaction of the board and management, and the identification, evaluation and mitigation of risks, while adhering to internal and external requirements necessary to achieve the organisation's objectives"*.

3.2 SOCs and their relevance in the South African context

Within the South African context state-owned companies are public entities established by statute, by national or provincial government departments, or by municipalities, and registered in terms of the Companies Act no 71 of 2008 (PwC 2011:4). In terms of the Public Finance Management (PFMA), Act no 1 of 1999, and the Municipal Finance Management Act (MFMA), Act no 56 of 2003, the government has ownership and control of SOCs. SOCs are listed in either the PFMA's Schedule 2 or 3, or are owned by a municipality (PwC 2011:4). In the South African context, PwC (2011:2) and Bouwman (2010:26) observe that SOCs operate in strategic sectors and play a critical role in infrastructure development, job creation, skills development, and economic and social transformation (PwC 2011:2). In addition, Bouwman (2010:26) emphasises the fact that non-performance by SOCs results in a drain on public resources and inhibits the economy's growth prospects. As outlined in the National Development Plan, for SOCs to achieve their objectives, GRC plays a critical role in ensuring accountability. SOCs are subject to complex governance structures (PwC 2011:4) similar to private companies, and this complexity makes the functioning of GRC in SOCs an important area for research. The increase in fraud and corruption and the misuse of public resources within SOCs has been attributed to poor GRC practices (PwC 2011:6).

3.3 State of GRC in SOCs

Implementation of GRC principles and protocols has become highly relevant for SOCs, as they are under increasingly intense scrutiny from the public and from government's oversight and regulatory bodies. Through implementation of the "Protocol on Corporate Governance", SOCs are embracing the "King Code of Governance Principles" (King III), amongst other best practices (Nkonki 2013:3). SOCs are thus making an effort to address GRC challenges in their organisations through intensifying focus on the management of risk, compliance with laws, codes, rules and standards, and by ensuring that the internal audit function is present and operational. A 2011 study conducted by PriceWaterhouseCoopers (PwC 2011:5) identified inadequate governance frameworks, poorly developed reporting and operational structures, and general ignorance of the regulatory environment as the primary causes of poor performance and lack of service delivery by SOCs.

3.4 GRC Maturity Models

Embedding GRC becomes achievable once an understanding of the GRC maturity level of the organisation has been obtained. Maturity models inform the organisation of the appropriate processes and tools to maintain the current and achieve future stages of maturity (Proviti 2013:5). While there is a multitude of literature available on different GRC maturity models (Nissen & Marekfia 2014:63; Batenburg, Neppelenbroek & Shahim 2014:47), every organisation needs to define the meaning of GRC in their own context (Thomson Reuters 2012:4). However, the most widely endorsed definition of GRC is that provided by the Open Compliance and Ethics Group (Thomson Reuters 2012:4; Mitchell & Switzer 2009:35). In this regard, the GRC maturity model, as outlined in the Open Compliance and Ethics Group GRC Capability Model (Mitchell and Switzer 2009:35) will be utilised for this study's comparison of SOCs' maturity models. The elements of the Open Compliance and Ethics Group GRC maturity model are outlined in Table 1 below. According to Tadewald (2014:10), the choice of GRC maturity model determines the processes needed, and ultimately the success of the entity's efforts, to integrate or embed GRC protocols.

The use of a GRC maturity model enables organisations to plan, monitor, and assess their implementation of GRC (Tadewald 2014:16). As is apparent in Table 1 below, at lower levels of maturity GRC efforts operate in silos as and when needed, while at higher levels of maturity there is a steady increase in integration and embedding of GRC within the entity. The GRC maturity model enables the organisation to identify gaps that exist between current practices and the desired maturity level. Using the OCEG GRC maturity model, the Unaware, Fragmented, and Integrated levels of maturity all indicate that GRC functions and processes are siloed, operating in isolation and without a holistic, company-wide view of risk and compliance (Rasmussen

2012:8). The Aligned and Optimised Platform maturity levels indicate that GRC processes are increasingly integrated, as indicated by the presence of an entity-wide GRC strategy with common GRC approaches, frameworks, and technology architecture, and the automatic sharing of information (Rasmussen 2012:8).

Table 1: Open compliance and ethics group (OCEG) GRC maturity model

Level 1 Unaware	Level 2 Fragmented	Level 3 Integrated	Level 4 Aligned	Level 5 Optimised platform
Governance, risk and compliance interdependencies are not understood by business. • Approach to technology is ad hoc and technology is non-existent. • Risk and compliance information is managed in documents and spreadsheets. • Information is not available, let alone shared. • Success is not measured. • GRC components operate in isolation. Business management characterised by reactive and non-integrated approaches. • Redundancies are widespread. • Few if any resources are allocated to risk and compliance. • Risk and compliance issues are addressed in a reactive mode: assessments only performed when forced to. • There is no ownership or monitoring of risk and compliance, and certainly no integration of risk and compliance information and processes, even at the function level. • Risk, compliance and controls are documented and maintained only as-needed. • There is no trending or analytics to track the state of risk and compliance.	Limited understanding of governance, risk and compliance interdependencies; no common platform for GRC provided. • Tactical, siloed approach to technology and systems, without integration. • There is some use of risk and compliance technology, but no integration or sharing of information and processes at function level. • The organization struggles with risk and compliance information that is trapped in silos' data-bases, spreadsheets and documents. • Measurement and trending is limited, consumes resources and takes a lot of time because of the scattered nature of risk and compliance information. • Approach not driven by risk. • Redundancy controls still minimal. • Relies on inefficient and labour intensive testing. • "Reactive" approach to managing control issues. • Risk and compliance is tactical and siloed (isolated) within the functions. • There is the beginning of accountability for risk and compliance. • Risk and compliance assessments are project-focused, not an ongoing effort of continuous monitoring.	The need to integrate GRC systems is recognised as the way to provide better information and results. • Existence of a common GRC platform and approach at function level. • Integrated GRC approach has not yet expanded as a strategy across multiple functions. • There are defined processes and a single strategy for GRC at the business function level. • There is an integrated information architecture supported by appropriate technology, and there is ongoing reporting, accountability, and oversight for risk and compliance functions. • Risk and control "owners" are defined and held accountable. • Information is shared across the enterprise. • GRC benefits are measured. • There are established processes for and regular assessments of risk and compliance. • The business can readily trend, monitor and report on GRC at any time and across periods, without significant inefficiencies.	Governance, risk and compliance interdependencies are understood and aligned. • There is a defined GRC strategy that crosses several or all GRC functions across the business. • Silos of GRC have effectively been eliminated, though there may remain some holdouts. • There is a common process, technology and information architecture supporting GRC across the business. • Business benefits are measured. • There is coordination of efforts to identify risks, assess exposure and prioritise actions. • Clear accountability and ownership of risk and control has been established across the organization. • The business is able to trend and report on GRC across all business functions.	A common language and set of metrics to continuously improve the GRC platform now exists. • There is a cohesive GRC strategy that is integrated throughout the business. • GRC technology is fully integrated. • GRC is embedded in all business systems. • The GRC strategy is supported and understood by the board and executive management. • Complete visibility to risk exposure and performance. • Identification of GRC expectations is part of annual strategic planning process. • GRC is understood, measured, and monitored in the context of business performance, strategy and objective management. • Continuous measurement and monitoring of risk and compliance in the context of the business and performance is performed.

3.5 Embedding GRC in an organisation

The objective of embedding GRC in an organisation is to remove the silo (ad hoc and isolated) approach to risk management and control (Balachandran & Sundar 2013:41). The process starts by achieving an understanding of the entity's current level of GRC maturity. Tadewald (2014:16) states that the use of a model enables organisations to understand their present state of GRC, from which point it is possible to manage the path to achieving the desired state of GRC. Embedding of GRC activities, to ensure that they are at the centre of decision-making, is a long-term process (Anon 2011:39). This requires knowledge of the entity's current maturity level, from which point the model can be used to direct management's strategy, processes, and action plans to achieve the preferred level of integration.

The process of embedding GRC (as with any business venture) starts with developing a strategy that includes clear objectives, goals, and vision (Frigo & Anderson 2009b:37). Thereafter, obtaining buy-in from the executive management and the board is vital (Proviti 2009:16; Anon 2011:39). Once a better understanding of GRC has been achieved by the board and senior management integration proceeds more efficiently and effectively because roles and relationships are more clearly understood and defined (Raths 2011:19; Frigo & Anderson 2009a:6; Anon 2011:39). This also ensures that GRC is managed effectively, delivers the required stakeholder value and sustains profitability (Anand 2010:57). To coordinate the implementation of the strategy, the board must appoint a committee that is representative of all those affected by GRC implementation (Proviti 2009:16). The committee should act as the single reference point for GRC issues, which will ultimately reduce costs and enable the effective embedding of the GRC processes (Greengard 2011:23).

Identification of individual GRC functions and components, and an understanding of the interaction between them (Frigo & Anderson 2009a:20; Anon 2011:39), is the next step in embedding the functions. Knowing where and when to integrate these components (Pickett 2011:82) is a critical step in embedding the process and achieving the required return on investment. Thereafter, the processes should be aligned to the context of the organisation (Hoon 2011:22). Agreement on a common GRC framework, risk language, and taxonomy (Phalke 2009:39; Pickett 2011:233) follows the identification of the required GRC functions.

According to the strategic governance, risk and compliance framework, the key elements that should be included in a GRC framework are: legal, compliance, safety, finance, internal audit, and information technology (Frigo & Anderson 2009a:20). Half the battle is won when there is an agreement on a common framework (Mccleen, as quoted by Raths 2011:19). The absence of a common framework has been identified as one of the key barriers to embedding GRC (Proviti 2009:15). Once the common framework and common language have been established, the definition of culture and philosophy follows (Balachandran & Sundar 2013:40). Tailoring the GRC initiatives to the organisational culture and governance structures ensures harmony (Frigo & Anderson 2009b:34).

To enable a coordinated strategy, it is essential to identify the different information technology systems and budgets present within the silo approach to GRC (Anon 2010:29). Thereafter, automation of key GRC processes enables the organisation to achieve a holistic and real-time view of GRC activities (Anderson 2011:60; Phalke 2009:39; Carpenter 2012:1; Greengard 2011:23). Technology is thus the backbone of, and key to, achieving GRC coordination and integration (Balachandran & Sundar 2013:41; Anand 2010:58). In summary, effective GRC revolves around having the right tools and technology, and well-defined processes (Greengard 2011:24).

To successfully embed GRC activities requires a coherent GRC implementation strategy and the presence of GRC "champions" (Konstans *et al* 2011:57). The process also requires entity-wide agreement on common operational frameworks, language, terms and methodologies (Raths 2011:19; Pickett 2011:233). GRC is only effectively embedded if it is driven from board level and cascades down throughout all levels of the organisation.

3.6 The role of the internal audit function in embedding GRC activities

Despite pressures to become compliant and to reduce costs, most organisations still find themselves managing their GRC activities in a fragmentary and uncoordinated manner, resulting in raised costs and an increased risk of regulatory non-compliance (Rasmussen 2012:3; Hoon 2011:22; Anderson 2011: 60). This creates an opportunity for the internal audit function to make a difference. Internal auditors add more value when focusing on management concerns (Pickett 2011:84). In light of the value proposition of internal auditing, internal auditors should be encouraged to move beyond merely providing assurance services, and should spend more time providing management with insight and recommendations (Chambers 2014:73) on effectively embedding GRC. Due to their strategic mandate and their good understanding of the organisation, internal auditors are well positioned to broaden their role (KPMG 2007) to assist in embedding GRC. This starts by playing an integral part in the combined assurance model, as recommended by King III (IODSA 2009:96). As defined by King III, combined assurance consists of coordinating and aligning internal and external assurance processes to maximise risk and governance oversight and control efficiencies (IODSA 2009:62). As internal assurance providers, internal auditors play a pivotal role in ensuring that GRC activities are embedded in the organisation.

However, the fact that internal audit is required to maintain independence and objectivity (Fraser & Henry 2007:393), raises the question of conflict of interest, should it become too involved in championing GRC activities. In the interest of protecting their independence, the IIA's *International Standards for the Professional Practice of Internal Auditing (Standards),*sets out assurance and consulting roles for internal audit in relation to GRC (IIA 2013). While internal auditors play an active role in such activities, this role should always be considered in relation to its potential to erode their independence.

In line with the IIA's *Standards,* internal audit's role can include the provision of both consulting and assurance services (IIA 2013). Internal auditors achieve the objectives of their mandate by being active role players (Pickett 2011:42), and in the same vein can also effect GRC benefits (Frigo & Anderson 2009b:36). These dual roles include improving value protection and increasing value creation (KPMG 2007). Both forms of value will be created when internal audit definitively answers the question: why does GRC matter to internal audit? By providing practical support to stakeholders, internal auditors demonstrate the role they play in embedding GRC (Chambers 2014:74). Below are key consulting roles that internal auditors perform to ensure that GRC activities are embedded:

- Assist management to make a business case for GRC integration, by providing evidence on how the existing, individual components of GRC are already supporting business performance (albeit sub-optimally). This gives the internal auditors an opportunity to better understand the organisation's GRC processes. Steffee (2012:11) asserts that, through this process, internal auditors can improve their audit processes and bridge the gaps that exist between the GRC activities;

- Spearhead the development of a common GRC definition, frame of reference, and language (Marks 2011);
- Assess and review the development and implementation of GRC structures, and educate management on the process (Frigo & Anderson 2009b:37). Through this assessment, possible challenges that are hindering or could in future hinder the achievement of GRC benefits will be identified;
- Provide a reliable, objective, and independent assessment of the design and effectiveness of GRC activities and their totality and integrity (KPMG 2012; Rasmussen 2009:61).
- Advise management on, initiate, and/or participate in, GRC projects to ensure the benefits of GRC are achieved (Frigo & Anderson 2009b:36);
- Advocate the ownership of accountability within and for the GRC processes by acting as advisers to senior management and the board (Davis & Lukomnik 2010:28);
- Develop measures and metrics that will be used by organisations to gauge GRC success (Konstans *et al* 2011:57);
- Spearhead the creation of forums and processes for GRC functions to build relationships that will improve sharing of knowledge and risk management techniques (Meiselman 2007:40);
- Facilitate and guide management on GRC activities and processes (Pickett 2011:84). The aim is to ensure that management and the board see that embedding GRC is more than compliance with regulations (Anon 2011:39); and
- Coordinate GRC functions by assisting management to implement GRC activities throughout the organisation, and to identify areas for further development (Frigo & Anderson 2009b:34). This also includes working together with executives to prioritise problems related to GRC implementation (Marks 2011).

Overall, it would seem that value is created when internal audit moves beyond providing assurance to embrace a broader role of influencing and improving how GRC activities are managed, before they become challenges (KPMG 2007). Understanding the interrelationship between business' three lines of defense (Tadewald 2014:12) should broaden the role internal audit ought to perform. In addition, internal auditors are also able to provide assurance on the risks associated with the continued use of siloed and fragmented GRC processes (Marks 2011).

4 RESULTS AND DISCUSSIONS

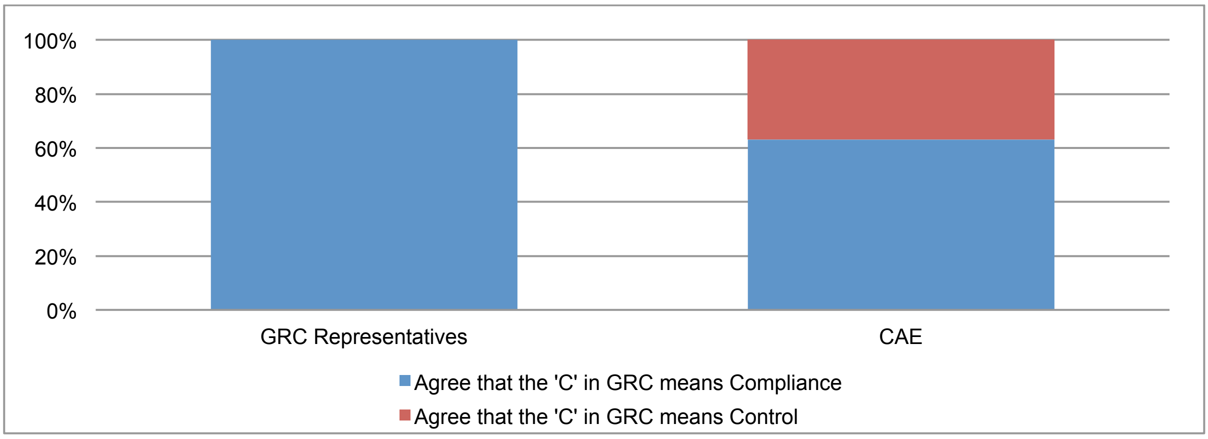
The results of the study will be analysed and discussed under the following subheadings:

- Understanding the GRC concept;
- GRC maturity levels in the selected SOCs;
- Embedding GRC and the role played by internal audit;
- How the internal audit function assists SOCs to progress to higher GRC maturity levels;
- Internal audit's challenges when attempting to assist organisations to embed GRC; and
- Lessons learnt that could be shared with internal audit functions in other SOCs.

Understanding the GRC concept

As outlined in Figure 1 below, 67% of CAEs agreed that the element 'C' in GRC means compliance while 33% of CAEs stated that, according to the International Standards for The Professional Practice of Internal Auditing (Standards), 'C' means Control. 100% of GRC representatives (Head of Compliance, Risk Manager, GRC Project Manager) agreed that 'C' means compliance. In line with the literature, there is no consensus on the meaning of 'C' in GRC.

Figure 1: Understanding the 'C' in GRC

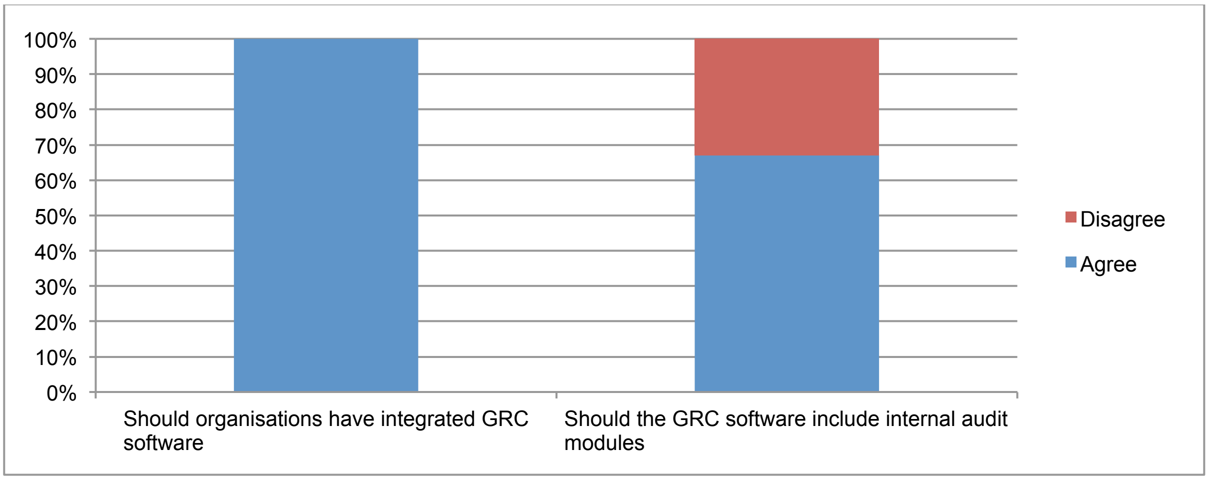


There was 100% consensus that GRC functions are there to ensure that businesses achieve their objectives. The GRC Project Manager for SOC A succinctly emphasised that to understand GRC, one first has to understand the value of each of the individual GRC functions before one can understand their collective value. 67% of CAEs held the view that everything starts with governance, as it is the key pillar for GRC. Governance is the umbrella concept within which risk management provides the key function. Compliance is a component of risk management, and all three aspects must be aligned. The CAE of SOC B stated that unless these three elements operate at a mature level an organisation would struggle to achieve its objectives. The results of the study indicate that 67% of CAEs and 100% of GRC representatives involved in GRC functions have the same understanding of GRC. The results of the study are in line with literature, as Proviti (2009:15); Frigo and Anderson (2009b34); and Mccleen, (as quoted by Raths 2011:19), state that having the same understanding on GRC principles clears barriers to effectively embedding GRC.

The study results show that 100% of CAEs hold the view that the internal audit function is not part of the GRC functions. The CAEs are of the opinion that the internal audit function should be independent of all GRC functions, to enable them to provide truly independent assurance and consulting services. The GRC Project Manager for SOC A shared the same understanding, adding though, that within their organisation they do not call it GRC but Internal Audit, Governance, Risk and Compliance (IGRC). However, this view is contrary to the strategic governance, risk, and compliance framework (Frigo & Anderson 2009b: 34) and the GRC Capability Model (Mitchell and Switzer 2009), which state that the internal audit function is a key component of the GRC activities and processes.

As outlined in Figure 2, below, there was 100% consensus amongst CAEs that having integrated GRC software was essential, thus allowing internal audit and the GRC functions access to the same, shared information set.

Figure 2: CAEs views on GRC software



However, 67% of the CAEs felt that the internal audit function should have its own standalone audit software, as internal audit also has access to sensitive and confidential company information. 33% of the CAEs did not object to internal audit modules being part of the GRC software. Later in the interviews,100% of CAEs indicated that if internal audit modules are part of the integrated GRC software system, this compromises their objectivity and thus their ability to provide assurance on the integrated software. On the other hand, SOC B's CAE expressed the view that if an integrated GRC software system is implemented, it should be customised to give the internal audit function access to information from GRC functions, while limiting GRC functions' access to internal audit's modules. Although the literature does not specify whether an internal audit module should be part of an integrated GRC software system, according to Proviti (2009:15), Greengard (2011:23), and Anand (2010:58), a common, integrated GRC software solution for all functions enables information sharing and coordination of GRC activities. In light of this, this study suggests that the internal audit module should be part of the integrated GRC software system.

GRC maturity level in the selected SOCs

Table 2, below, presents respondents' views on the maturity levels of SOCs' GRC processes. These still appear to be essentially siloed, as maturity levels span the spectrum from "fragmented, "through "integrated, "to "aligned".

The CAEs for SOCs B and C confirmed that the maturity levels for their entities are between "fragmented" and "integrated". SOC A's CAE and the GRC Project Manager have different understandings of their SOC's GRC maturity level. The CAE sees it as "integrated" while the GRC Project Manager views it as falling between "fragmented" and "integrated". The differing perspectives on GRC maturity stages expressed by internal auditors and those with GRC management responsibilities suggests that a full embedding of GRC is yet to take place in SOCs. This also supports the view that within an organisation one element of the GRC functions might well be "mature," while the others are still only "evolving". The CAE for SOC B was unusually specific, stating that their maturity level was 75% "fragmented" and 25% "integrated," while SOC B's GRC representative's view was that it was "integrated". The differing views within the same organisation show that GRC is not fully embedded in this entity. There was consensus amongst all interviewees that the GRC maturity level for SOCs in general is still "fragmented". The inference is that within SOCs, GRC is still seen as three individual functions and not as an integrated whole. Although SOCs A and C have executives dedicated to overseeing all GRC functions, their maturity levels are still between "fragmented" and "integrated". The GRC Project Manager for SOC A stated that, while their GRC functions are effective individually, what is lacking is the integration of these siloed functions that would enable the organisation to develop a holistic business perspective on risk and compliance. The results of the study are in line with the views put forward by Hoon (2011:22) and Anderson (2011:60), that the current GRC processes in organisations is still best described as 'fragmented' and needs to evolve.

Table 2: GRC maturity levels of SOCs

Research questions	SOC A		SOC B		SOC C	
	CAE	GRC project manager	CAE	Senior risk manager	CAE	Head of compliance
What is your organisation's current GRC maturity level?	Integrated	Between integrated and aligned	Between fragmented and integrated	Integrated	Between fragmented and integrated	Between fragmented and integrated
What is the organisation's desired GRC maturity level?	Aligned	Aligned	Aligned	Aligned	Aligned	Aligned
Based on our understanding of SOCs what is the general SOCs GRC maturity level?	Fragmented	Fragmented	Fragmented	Fragmented	Fragmented	Fragmented

Note: This table is based on responses to questions on the current and desired GRC maturity levels of the interviewed SOC GRC representatives, and their views on the maturity levels of SOCs in general.

Embedding GRC and the role played by internal audit

Study results show that 100% of CAEs share a common understanding that the GRC maturity level of an organisation informs internal auditors on what role they should play. However, the reality is that the GRC maturity assessment is still conducted separately for each of the individual GRC elements, rather than holistically. Stated slightly differently, 100% of CAEs agreed that, while an organisation might have a low overall GRC maturity level, the maturity level of an individual function (e.g. risk management) might be significantly different. SOC A's CAE explained that their internal audit function provides consulting services to parts of the organisation where there are low maturity levels, and assurance where maturity levels are somewhat higher.

100% of the CAEs for the three SOCs agreed that internal audit's role in embedding GRC principles starts with showing the practical benefits of an integrated GRC approach. SOC C's CAE emphasised that, for this company, the internal audit function's involvement in embedding GRC starts with proving its business case to management and the other assurance providers. That is, it wins over stakeholders through showing the benefits of fully embedded, integrated, and coordinated GRC functions.

There was consensus amongst CAEs that their role in embedding GRC is through spearheading and coordinating the constituent elements of the combined assurance model. This view is in line with King III, which advocates for the internal audit function to spearhead combined assurance. SOC C's CAE stated that in driving the combined assurance model they intend to achieve the following:

- to get business to understand the impact of not resolving audit findings;
- to get business to see the link between unresolved findings and heightened risks;
- to change the mind-set that resolving issues is a management function (not an operational matter); and
- to bring about a change of attitude towards risk management so that it becomes integrated and owned by the entire business.

In addition to generally agreeing with the above,

- SOC C's CAE's role was to work with other assurance providers to identify the points of contact and overlap between risk management and compliance functions, and to plan the embedding process;
- SOC A's CAE considered his role to include identification and elimination of duplicated efforts, and introducing assurance in areas where no assurance is as yet being provided; and
- SOC A's CAE saw his role as obtaining an understanding of challenges timeously and responding appropriately.

In addition, SOC C's CAE explained that the internal auditors play an active role in embedding GRC functions in the organisation through spearheading meetings of the combined assurance steering committee. Obstacles to the embedding of GRC processes are identified and addressed by the combined assurance steering committee at these meetings. Effectively, the coordination of the efforts of the constituent functions of the combined assurance model results in GRC processes being embedded. SOC B's CAE stated that their internal audit function influences the process of embedding GRC functions, in line with the generally accepted combined assurance model, by being represented at every executive and operational committee level within the organisation.

In addition, SOC B's CAE stated that their internal audit function also plays a part in embedding GRC through adopting a formal risk-based approach to their duties that consistently identifies areas of weaknesses and indifferent controls. SOC C's CAE explained that their audit function is currently assisting their organisation in embedding GRC by involving staff from operational areas as guest auditors, by having joint audits, and by switching roles with other assurance providers. For example, having the internal audit function working together with compliance functions at their regional offices, to monitor compliance, enhances mutual understanding and improves operational efficiency. According to SOC C's CAE, because of this approach executives at regional offices no longer accept individual audits when assurance providers visit their offices. They insist on joint audits that involve all assurance providers.

The general view expressed by interviewees was that embedding GRC functions is at the centre of achieving core business goals. The GRC project manager for SOC A succinctly stated that the key to embedding these functions is the alignment of component GRC activities, without diluting the individuality of each function. The results of the study show that the internal audit function is best positioned to assess the effectiveness of GRC functions and to play an active role in the embedding of GRC processes. This view is supported by KPMG (2007), Pickett (2011:84), Chambers (2014:74), and Steffee (2012:11), who advocate for internal auditors to provide practical support to stakeholders, to ensure that GRC processes are embedded.

How internal auditors assist SOCs to progress to higher GRC maturity levels

When asked what their roles were in assisting their organisations to achieve higher GRC maturity levels, 100% of the CAEs agreed that they have had to initiate the processes and to motivate for a solution to the GRC integration and embedding challenge. Their motivation has been that a GRC solution will eliminate the current challenges and risks posed by manually integrating data, and that risks and compliance issues will be managed more effectively and transparently. However, the CAE for SOC C noted that it was the maturity of the internal audit function that was key to defining the role they play in assisting organisations to achieve higher GRC maturity levels. In other words, the internal audit function must have the prerequisite tools available before they can offer to assist the organisation to improve its maturity level; i.e., it must be at a higher level of "maturity" than the functions it is offering to assist.

The CAEs in SOCs B and C, and SOC A's GRC Project Manager each acknowledged that internal audit is able to assist their organisations to move to a higher maturity level of GRC integration through fully embedding the combined assurance model, and strengthening the combined assurance approach, by ensuring that the existing GRC system is measurable. This enables the business to conform to a common GRC model, with shared methodologies and frameworks. The GRC Project Manager for SOC A pointed out that, as their organisation is currently implementing an integrated GRC solution, the internal audit function (as the coordinator of combined assurance) has the opportunity to provide assurance on the implementation of the GRC system. Consistent with current views in the literature, a single source of GRC information enables the internal auditors to play a critical role in embedding GRC, as they have access to consistent, real-time risk and compliance information (Pickett 2011:42; Marks 2011; Steffee 2012:11).

Furthermore, according to SOC C's CAE, the key to embedding GRC is to proactively achieve integration for areas that fall within the GRC spheres of business. SOC B's CAE noted that in addition to fulfilling their normal internal audit roles, they also have to act as agents of change, given that they have a good understanding of GRC processes and are experts on the interrelationships of the organisation's divisions. Internal auditors are the self-professed best agents to bring about change within the organisation. SOC A's CAE explained that internal audit's role in assisting the organisation to move to a higher GRC maturity level starts by raising awareness amongst executives that integration of GRC is a process that requires the participation of all executives. The current situation, where only one executive champions the process, is proving to be less than optimally effective. Thus, executives need to be guided to achieve an understanding of what GRC entails, as the first step to achieving their endorsement of, and participation in, the integration and embedding processes. As stated by Proviti (2009:10) and Anon (2011:39), the success in embedding GRC processes is dependent on buy-in from executive management and the Board.

Internal audit's challenges when attempting to assist organisations to embed GRC

One CAE explained that the main challenge to the embedding of GRC is that the board's oversight bodies are not aggressive enough in their efforts to reverse the mediocre performances of those managers already supposedly implementing GRC. In addition, there appears to be an attitude of non-accountability, and a lack of support from executive leadership, that hinders the internal audit function's efforts to effectively fulfil its roles. According to another CAE, there are still some gaps in their executives' understanding of GRC as some executives still see implementation of GRC as hindering them in the performance of their "real" work.

The results of the interviews with the three SOCs support those of Chartis Research Ltd (2014:5), which identified that GRC is failing, both at an integration level and an operational level, because the focus has tended to favour processes and systems, while overlooking people and their behaviours. Focusing on the people that implement the business processes and systems is critical to the overall success of GRC (Chartis Research Ltd 2014:5).

Lessons learnt that could be shared with internal audit functions in other SOCs.

According to one of the CAEs, the lesson learnt is that the internal audit function must recognise when their auditing professionalism gets in the way of the need to see the business from management's viewpoint. Doing so would then enable the internal auditors to demonstrate the merit of their business case and effectively show the benefits of GRC. Another CAE stated that SOCs should also be evaluated according to the same GRC maturity model as private companies, as SOCs are also required to comply with King III.

Another of the CAEs explained that, in the process of embedding GRC, one has to take management along at the right pace so as not to lose them. In addition, the definitions should be clear and well understood [by the person leading the embedding process], and there should be an agreement on the proposed deployment of technology to be used for GRC, as people (particularly those tasked with performing routine duties) do not like unilateral impositions. According to SOC A's CAE, getting buy-in from the top is the key to successfully embedding GRC processes.

5 CONCLUSION

Effective embedding of GRC processes and principles is critical to the success of any organisation. Internal auditors and those with GRC management responsibilities generally have a similar understanding of the GRC concepts, of maturity, and of how the processes are embedded. Having the same understanding of GRC principles and processes within an organisation is a key element to successfully embedding them. Overall, GRC in SOCs is still on the lower end of the GRC maturity model, i.e., "fragmented" and "integrated". Internal audit's role in embedding GRC is informed by the GRC maturity levels of the individual component functions and through actively showing management the benefits of implementing an integrated GRC protocol. Through leading and coordinating company-wide efforts to achieve combined assurance, internal audit functions are actively involved in embedding GRC processes. All of these efforts will result in SOCs improving their maturity levels. The challenges to and lessons learnt from efforts to embed GRC hinge on a lack of executive support, difficulty in achieving agreement on key definitions, and the choice of technology.

In conclusion, this study provides insight into GRC practices in South African SOCs, and the role of their internal audit functions in embedding GRC. The strength of this study is that it has highlighted that the internal audit function's role in embedding GRC is effectively achieved through driving combined assurance. Through establishing combined assurance forums to implement and embed the combined assurance framework principles, the internal audit function assists the organisation to improve its GRC maturity levels. It should however be noted that internal audit's role in embedding GRC goes beyond identifying ineffective risk management, breaches in compliance, and governance failures. The findings of the study also noted that SOCs are required to implement the same corporate governance principles as private sector companies. This also endorses the importance of GRC for SOCs. The SOCs selected for this study can also be used by other SOCs to benchmark themselves and to develop plans for the rollout of their GRC programmes, in order to progress to higher maturity levels.

Although there are various GRC maturity models, the majority are industry- and organisation-specific, and not all models are applicable or adaptable to all organisations. Having said this, from the literature reviewed there are apparently no GRC-specific maturity models that are aligned to the operating environments of SOCs. To meet current and future challenges the internal audit profession would benefit by exploring the GRC maturity model within the context of the SOC environment. This will enable SOCs (and the public sector in general) to measure the maturity levels of the constituent functions within GRC, and to assess the level of collaboration between the different GRC functions. In addition there is also room to study the effectiveness of the combined assurance model as a tool for embedding GRC principles in the business. Furthermore, research is still required to explore GRC implementation in the rest of South Africa's SOCs, and to identify the key challenges faced in this process. Of particular interest for future study is the level of maturity of governance, risk, and compliance management already achieved within SOCs, and the impact of this maturity level on the roles (expected and actual) of internal audit. Such research would provide a useful roadmap for the achievement of complete integration of GRC, and thus lead to improved service delivery, governance, and performance outcomes in SOCs and the public sector in general.

REFERENCES

Abdolmohammadi, M.J., Ramamoorti, S. & Sarens, G. 2013. *CAE Strategic Relationships: Building rapport with the executive suite*. The Institute of Internal Auditors Research Foundation. Altamonte Springs, Florida.

Anand. S. 2010. Technology and the Integration of Governance, Risk Management and Compliance. *Financial executive*, December, 12:57-58.

Anderson. S. 2011. Automating governance, risk and compliance. *Financial Executive*, 27(5):60-63.

Anon. 2010. US insurers taking up GRC in budget drive. *Operational Risk & Regulation*, 11(7):29.

Anon. 2011. Pushing for GRC. *Operational Risk & Regulation*, 12(7):38-41.

Balachandran, B.V. & Sundar, K.S. 2013. Governance, risk, and compliance: The value driver for good corporate governance. *Cost Management*, 27(6):39-47.

Batenburg, R., Neppelenbroek, M. & Shahim, A. 2014. A maturity model for governance, risk management and compliance in hospitals. *Journal of Hospital Administration*, 3(4):43-52.

Bloomberg, L.D. & Volpe, M. 2012. *Completing your qualitative dissertation – A road map from beginning to end*. 2nd edition. Sage Publications. Los Angeles.

Boultwood, B. 2013. *The GRC value proposition. Global Association of Risk Professionals.* [Online]. www.garp.org/risk-news-and.../the-grc-value-proposition.aspx (Accessed: 6 January 2014).

Bouwman, N. 2010. Governing state-owned enterprises. *Without prejudice*, December, 10(11):26-28.

Cadbury Report, A. 1992. *Report of the committee on the financial aspects of corporate governance.* The Committee on the Financial Aspects of Corporate Governance. Gee and Company Limited. London.

Carpenter, B. 2012. Award-Winning GRC*. Internal Auditor*, August, 69(4):17.

Chambers, R.F. 2014. *Lessons learned on the audit trail*. The Institute of Internal Auditors Research Foundation. Altamonte Springs, Florida.

Chartis Research Ltd. 2014. *Enterprise GRC Solutions 2014: Time for GFRC?* MetricStream Vendor Highlights. [Online]. http//www.chartis-research.com (Accessed: 7 July 2014).

Coetzee, G.P. 2010. *A risk-based audit model for internal audit engagements*. Unpublished 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.* Sponsoring Organisations of the Treadway Commission. Jersey City. New Jersey.

Companies Act no 71 of 2008. Pretoria: Government Printers.

Creswell, J.W. & Clark, V.L.P. 2007. *Designing and conducting mixed methods research.* Thousand oaks, CA: Sage.

Davis, S. & Lukomnik, J. 2010. Enabling good governance. *Internal Auditor*, April, 67(2):28-29.

Ernst & Young. 2013. EY's Excellence in Integrated Reporting Awards 2013. *A survey of integrated reports from South Africa's top 100 JSE listed companies and top 10 state owned companies.* [Online]. http://www.ey.com/Publication/vwLUAssets/EYs_Excellence_in_Integrated_Reporting_Awards_2013/$FILE/EY%20Excellence%20in%20Integrated%20Reporting.pdf (Accessed: 17 March 2014).

Fraser, I. & Henry, W. 2007. Embedding risk management: structures and approaches. *Managerial Auditing Journal*, 22(4):392-409.

Frigo, M.L. & Anderson, R.J. 2009a. Strategic Framework for Governance, Risk, and Compliance. *Strategic Finance*, February, 90(8):20-61.

Frigo, M.L. & Anderson, R.J. 2009b. 10 Strategic GRC: Steps to implementation*. Internal Auditor*, June, 10:33-37.

Greengard, S. 2011. The GRC Maze. *Baseline*, September/October, 112:20-24

Hoon, A. 2011. A holistic approach to GRC. *Accounting Today*, 25(7):22-25.

Institute of Directors Southern Africa.2009. *King Report on Governance for South Africa*. Johannesburg. Institute of Directors Southern Africa.

Institute of Risk Management, UK. 2002. *A Risk Management Standard*. [Online]. http://www.theirm.org/ publications/documents/ Risk_Management_ Standard _030820.pdf (Accessed: 10 July 2010).

International Federation of Accountants (IFAC). 2014. *International Framework: Good Governance in the Public Sector – Supplement.* [Online]. https://www.ifac.org/sites/default/files/publications/files/International-Framework-Good-Governance-in-the-Public-Sector-supplement-IFAC-CIPFA-June-2014.pdf (Accessed:7 July 2014).

International Standards Organisation. 2009. ISO 31000: *Risk Management – Principles and Guidelines*, ISO. Geneva, Switzerland.

Konstans, C., Radhakrishnan, S., Switzer, C.S. & Williams, L.C. 2011. In search of ‘principled’ performance. *Financial Executive*, 27(10):55-57.

KPMG.2007. *The evolving role of internal audit: Value creation and preservation from an internal audit perspective*. [Online]. https://www.kpmg.com/ZA/en/IssuesAndInsights/ArticlesPublications/Risk-Compliance/Documents/The%20Evolving%20role%20of%20the%20Internal%20Auditor.pdf (Accessed: 7 June 2014).

KPMG. 2012. *A good offense is the best offense: Managing regulatory compliance with GRC.* [Online]. https://www.kpmg.com/US/en/IssuesAndInsights/ArticlesPublications/Documents/managing-regulatory-compliance-grc.pdf (Accessed: 7 June 2014).

Lamont, J. 2012. GRC: The upside of risk. *KMWorld,* October, 21(9):18-19

Marks, N. 2010. Defining GRC. *Internal auditor*, February:25-27.

Marks, N. 2011.*The GRC Survey: The results are in.* [Online]. http://normanmarks.wordpress.com/2011/02/01/the-grc-survey-the-results-are-in/ (Accessed: 23 July 2014).

McGraw, S. 2012. GRC focus: Keep your employees close and your auditors closer. *Compliance & Ethics Professional*, (March/April):28-29.

Meiselman, J. 2007. Risk, Governance and compliance trends for 2007. *Risk Management*, 54(2):40.

Metricstream. 2013. *The Future: Pervasive GRC*. [Online]. http://www.metricstream.com/pdf/whitepapers/Pervasive-GRC.pdf?alild=105897079 (Accessed: 6 January 2014).

Mitchell, S.L. & Switzer, C.S. 2009. *GRC Capability Model.* Red Book 2.0. Open Compliance & Ethics Group, Phoenix.

Municipal Finance Management Act (MFMA). 2003. *Act No 56 of 2003,* Pretoria: Government Printers.

Naidoo, R. 2009. *Corporate governance: An essential guide for South African Companies.* 2nd edition. Durban: LexisNexis.

National Treasury of South Africa. 2010. *Public Sector Risk Management Framework*. Pretoria: Government Printers.

Nissen, V. & Marekfia, W. 2014 The Development of a Data-Centred Conceptual Reference Model for Strategic GRC. *Management. Journal of Service Science and Management*, 7:63-76.

Nkonki Incorporated (Nkonki). 2013. *Insights into SOC* Integrated Reporting Trends in South Africa.* [Online]. http://www.nkonki.com/IR/publications.php?a=integrated-reports&page=insights-into-soc-integrated-reporting-trends-2013 (Accessed: 27 July 2014).

Organization for Economic Co-Operation and Development (OECD). 2004. *Principles of Corporate Governance.* [Online]. http://www.oecd.org/corporate/ca/corporate/governance/principles/31557724.pdf (Accessed: 3 July 2014).

Phalke, V. 2009. Breaking down silos for integrated Governance, Risk and Compliance. *Siliconindia*, February:39.

Pickett, K.H.S. 2011.*The essential guide to internal auditing*. 2nd edition. West Sussex: John Wiley & Sons.

Protiviti. 2009. *Key questions surrounding integrated GRC*. [Online]. http://www.protiviti.com/en-US/Documents/White-Papers/Risk-Solutions/Integrated_GRC.pdf (Accessed: 30 June 2014).

Protiviti. 2013. *Growing with Governance, Risk and Compliance (GRC) Solutions. Avoiding common pitfalls to maximise GRC solutions*. [Online]. http://www.protiviti.com/en-US/Documents/White-Papers/Risk-Solutions/Growing-With-GRC-Solutions-Protiviti.pdf (Accessed: 4 July 2014).

PricewaterhouseCoopers (PwC). 2011. Stated-owned enterprises: *Governance responsibility and accountability. Public Sector Working Group: Position Paper 3.* [Online]. http://c.ymcdn.com/sites/www.iodsa.co.za/resource/collection/879CAE6C-7B90-49F5-A983-28AECBCE196F/PSWG_Position_Paper_3_Governance_in_SOEs.pdf (Accessed: 30 June 2014).

Public Finance Management Act (PFMA). 1999. *Act No 1 of 1999*, Pretoria: Government Printers.

Rasmussen, M. 2009. An Enterprise GRC Framework. *Internal Auditor*, October, 10:61-65.

Rasmussen, M. 2012. GRC Maturity: *From Disorganized to Integrated Risk and Performance*. Corporate Integrity, LLC. [Online]. http://grc2020.com/2012/04/20/57grc-maturity-from-disorganized-to-integrated-risk-and-performance/ (Accessed: 31 July 2014).

Raths, D. 2011. The big picture. *KM World***,** 20(7):18-19.

Stanford, J. 2004. Curing the ethical malaise in corporate America: Organizational structure as the antidote. *Sam Advanced Management Journal*, *69*(3):14-21.

Steffee, S. 2012. GRC Conundrum. *Internal Auditor*, 69(2):11-13.

Steinberg, R.M. 2010. Common Questions about GRC and Some Answers. *Compliance Week*, September: 40-41.

Tadewald, J. 2014. GRC Integration: A conceptual Foundation Model for Success. *Management accounting quarterly*, Spring 2014,15(3):10-18.

Teddlie, C. & Yu, F. 2007. Mixed Methods Sampling: A Typology With Examples. *Journal of Mixed Methods Research*, 1:77, SAGE publications.

The Institute of Internal Auditors (IIA). 2013. *International Professional Practices Framework.* Altamonte Springs, FL, from the glossary.

The Institute of Internal Auditors Research Foundation (IIARF). 2013. *Contrasting GRC and ERM: Perceptions and Practices among Internal Auditors.* [Online]. http://www.theiia.org/bookstore/product/contrasting-grc-and-erm-perceptions-and-practices-among-internal-auditors-download-pdf-1751.cfm (Accessed:17 June 2014).

The Risk Management Institution of Australasia Limited (RMIA). 2012. *The role of the risk professional in leading the G in GRC*. [Online]. http://www.rmpartners.com.au/images/stories/Whitepapers/Risk%20Professionals%20 Leading%20the%20G%20in%20GRC.pdf (Accessed: 7 June 2014).

Thomson Reuters Accelus. 2012. Building a business case for governance, risk and compliance. [Online]. www.accelus.thomsonreuters.com/sites/default/files/GRC00015.pdf (Accessed: 9 August 2014).

Verschuren, P. & Doorewaard, H. 2010. *Designing a research project*, 2nd edition, The Haque: Netherlands.

Yin, R.K. 2009. *Case study research: Design and methods,* 4th edition. London: Sage Publications.

The Southern African Journal of Accountability and Auditing Research

Evolving Research

Mitigating strategies for sampling risks to enhance the reliability of the internal audit opinion

L A Smidt
Department of Auditing
Tshwane University of Technology

D S Lubbe
Centre of Accounting
University of the Free State

D P van der Nest
Department of Auditing
Tshwane University of Technology

G P Coetzee
Department of Auditing
Tshwane University of Technology

ABSTRACT

This article explores the mitigating strategies for risks associated with the use of sampling techniques that are implemented by internal audit functions in the banking sector of South Africa. Risks associated with audit sampling techniques may adversely impact the reliability of the internal audit opinion, which is used by various stakeholders when performing their decision-making duties. The research results indicate that respondents mostly implement in-house mitigating strategies to minimise the risks relating to the calculation of the sample size, the application of the sampling selection method and the evaluation of the sample results. External mitigating strategies are implemented to a lesser extent, and this situation should be explored by the respective respondents.

Key words

Banking industry; internal auditing; sampling techniques; sampling risks; mitigating strategies

1 INTRODUCTION

Internal auditing is well-represented in the banking industry. This is supported by the 2010 Common Body of Knowledge (CBOK) study conducted globally by the Institute of Internal Auditors (IIA), which reported that 30% (Alkafaji, Hussain, Khallaf & Munir 2010:35) of the nearly 13 500 respondents were employed in the financial sector, including banking. For South Africa, the corresponding figure was 15% (Coetzee, Fourie & Burnaby 2014:n.d.). The role of the internal audit function within the banking industry is defined and guided by numerous international "conventions", of which the two most significant are the IIA's International Standards for the Professional Practice of Internal Auditing (hereafter referred to as the *Standards*) (IIA 2012) and the Basel Committee's Supervisory Guideline on the Internal Audit Function in Banks (BIS 2012). In South Africa, the roles and requirements of internal audit functions are also described in the 2009 King Report on Governance for South Africa (hereafter referred to as King III Report) and the Banks Act respectively (South Africa 2007: S48(k)). These documents support the overall objective of internal auditing which is to assist management with the achievement of their objectives through an independent evaluation of the effectiveness of governance, risk management and control processes.

The objective of internal auditing is achieved by the performance of various assurance and consulting engagements performed. The final deliverable of an internal audit engagement is the internal auditors' Sreport: as its key deliverable, this should include the internal auditors' conclusion or opinion relating to the particular audit engagement objective (IIA 2012: S2410.A1). It is important that the opinion addresses the expectations of senior management, the board, and other stakeholders, and should be supported by sufficient, reliable, relevant, and useful evidence (IIA 2012:S2310; IIA 2012:S2410.A1). In addition, the Supervisor of South African banks (which is the South African Reserve Bank's Bank Supervision Department), the bank's board of directors, its audit committee, and its senior management are all key stakeholders that have rising expectations of the effectiveness of the internal audit function (South Africa 2007:S48 (v)(i); IOD 2009:95-100; Rezaee 2010:50; BIS 2012:15;

PwC 2012:18). As these key stakeholders indubitably place reliance on the internal audit opinion, the reliability thereof is thus vital.

As it is impossible for the internal audit function to provide assurance on each and every activity of the bank, internal auditors have to obtain a sample of the evidence upon which to base their opinion. Therefore, the *sampling plan*, *size* and *selection* (hereafter referred to as sampling technique) used by the internal auditor should be of such a nature that the opinion expressed is a reliable indication of the current and future state of the governance, risk management and control processes tested. In other words, the auditee should be able to interpret the results presented, and to apply the findings of the report, with confidence.

Risks associated with the application of sampling techniques that could have an adverse impact on the reliability of the internal audit opinion, are sampling risk and the selection bias, and their associated pitfalls. In order to provide reliable audit opinions, internal audit functions must successfully address these risks through their choice of sample techniques. As previously mentioned, internal auditing is well-represented in the South African banking industry. Therefore the objective of the study reported in this article is to identify mitigating strategies implemented by the internal audit functions of the South African banks in their efforts to overcome the risks associated with sampling techniques, in order to enhance the reliability of the internal audit opinion.

In the next section the research method is discussed, and this is followed by a literature review, research findings and a conclusion.

2 RESEARCH METHOD

A quantitative research methodology was followed: data was collected by means of a structured questionnaire which provided the quantitative data. Thereafter a follow-up interview was conducted in order to obtain clarity on questions that had been incompletely or ambiguously answered. This method was used to gather statistical data (using descriptive statistics) for analysis as limited literature is available regarding the mitigating strategies implemented by internal auditors when employing sampling techniques. Similarly, as far as the authors have been able to determine, no literature is available with regards to the sampling techniques employed by internal auditors within the banking industry.

The research population consisted of the Chief Audit Executives (CAEs) of in-house internal audit functions from all locally-controlled banks registered with the South African Central Bank (Reserve Bank), and, by virtue of this registration, were permitted to conduct the business of a bank in South Africa at the time the research was undertaken (see Annexure A for a list of these banks). The CAEs were contacted via e-mail and provided with a questionnaire to complete and return. Nine (9) questionnaires were completed and returned, producing an overall response rate of 90%. Although only 9 responses were obtained, firstly, it represents 90% of the locally controlled banking industry, and secondly, informative nonparametric statistical analysis may be conducted on such a small number, providing only descriptive statistics are used (Leedy & Ormrod 2005:252; Dickie 2014). Further studies could include other industries in South Africa, or be extended globally.

3 LITERATURE REVIEW

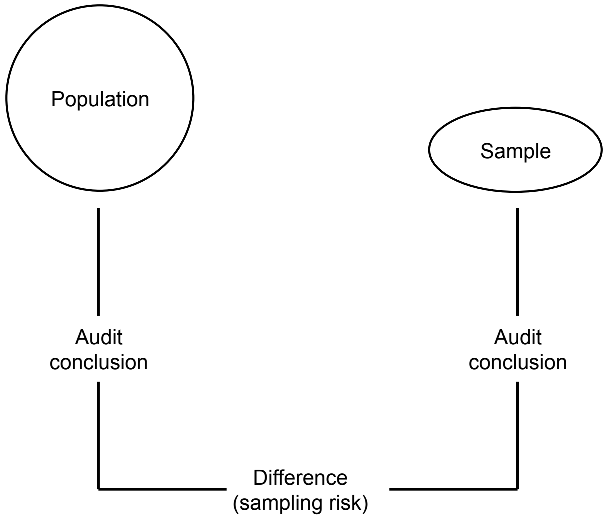
Audit sampling is a technique that relies on selecting a limited number of representative items from a much larger population, and examining these in detail. (IIA 2013:PA2320-3). Sampling techniques, furthermore, consist of statistical and non-statistical methods of selection. Statistical sampling employs probability-based techniques that enable the internal auditor to draw statistically backed inferences about the entire population under review, and it also allows for the calculation of sampling risk. Non-statistical sampling is a technique that is based purely on the auditor's professional judgment and does not make use of the laws of probability, and as such, inferences regarding the entire population under review cannot be made (Hitzig 2004:31; Maingot & Quon 2009:218). In this section the literature on risks associated with both statistical and non-statistical techniques, as well as potential mitigating strategies, are discussed.

3.1 Sampling risk

Sampling risk is the risk that the audit conclusion, derived from a sample, might be different from the conclusion that would have been reached if the entire audit population had been subject to the internal auditor's assessment (Apostolou 2004:13; Aghili 2011: 19; IIA 2013:PA2320-3). The representativeness of the sample will be questionable if the characteristics displayed in the sample are not a true representation of the audit population's characteristics. It is therefore important for the internal auditor to employ an appropriate sample selection method in order to ensure the sample characteristics display the population's characteristics, and therefore effectively achieve the engagement objective. Figure 1 provides a schematic view of sampling risk.

Sampling risk is most frequently associated with the use of statistical sampling techniques (IIA 2013: PA2320-3), and can be quantified (Stuart 2012:237). By way of contrast, sampling risk cannot be quantified if a non-statistical sampling technique is used (Crous, Lamprecht, Eilifsen, Messier, Glover & Douglas 2012: 238). Furthermore, there is a distinction between sampling risk for tests of controls, and for substantive tests. Sampling risk for substantive tests comprises (1) the risk of incorrectly rejecting a materially correct balance, and (2) the risk of incorrectly accepting a materially incorrect balance. The risk of incorrectly rejecting a materially correct balance will have an impact on the *efficiency* of the audit (necessitating additional time and procedures), as the internal auditor could conclude that a material misstatement does exist when in fact it does not. In contrast, the risk of incorrectly accepting a materially incorrect balance could lead to an *inappropriate audit opinion* as the auditor could conclude that a material misstatement does not exist when in fact it does (Apostolou 2004:13). Sampling risk for substantive tests is present when monetary values are tested, and is more widely used by the external auditor (IFAC 2012a:ISA530(5)(c)). Sampling techniques used in tests of controls are frequently used by internal auditors when conducting internal auditing engagements. As this study focused on the use of sampling techniques employed by internal audit functions in the South African banking industry, only the latter will be discussed hereafter.

Figure 1: Schematic view of sampling risk



Source: Sumners (2008:174)

The sampling techniques for tests of controls are intended to address the risk of over-estimating the control risk (i.e. the internal auditor places too little reliance on the operating effectiveness of controls), and/or the risk of underestimating the control risk (i.e. the internal auditor places too much reliance on the operating effectiveness of controls) (IIA 2013: PA2320-3). Although both these scenarios are applicable to an internal audit engagement, the internal auditor is mainly concerned with the risk associated with underestimating the control risk, as this could impact on the effectiveness of the audit and could lead to incorrect audit opinions. As an overreliance on internal controls could lead the internal auditor to conclude that the controls in place are effective and working as intended, when in fact they are not, this could have serious consequences on the *reliability* of the overall audit opinion. Conversely, the risk of over-estimating the control risk will have an adverse impact on the efficiency of the internal audit engagement, which is a risk with less serious consequences for internal auditors than would arise from underestimating control risk (Apostolou 2004:13; Aghili 2011:19). An under-reliance on internal controls could lead the internal auditor to conclude that controls are ineffective, when in fact they are effective. This under-reliance on controls can however be addressed through the use of additional audit procedures, but this will lead to the deployment of more audit resources and effort, and will therefore negatively impact on the audit's *efficiency* and increase the costs of performing the audit.

The internal auditor should also be aware of the risk of applying a sampling technique that is inappropriate or irrelevant for a specific internal audit engagement objective as this could lead to an inconclusive and/or incorrect outcome. For example, if the internal auditor uses a sample size that is too small, it may not be representative of the characteristics of the population: hence it may lead to an inconclusive outcome, and wasted audit effort (Moeller 2009:203). Furthermore the internal audit opinion may also be adversely impacted by risks not related to audit sampling: however, this situation does not form part of this study.

3.2 Sampling Bias

Whereas sampling risk is mostly associated with statistical sampling techniques, sampling bias is more commonly encountered with the use of non-statistical sampling techniques. Although the use of non-statistical sample selection methods is permitted by the professional standards, they should be used with caution as they have distinct limitations (IFAC 2012a:ISA530). The two most widely preferred non-statistical sampling techniques are haphazard sampling and block sampling.

Haphazard sampling is said to occur when the internal auditor selects items in an unstructured manner, without any conscious bias to specifically include or to exclude any items from the sample selection (Hall, Higson, Pierce, Price & Skousen 2012:102). The use of a haphazard sampling technique could however, still be susceptible to selection bias, a fact that has repeatedly been confirmed by numerous studies (Hall, Hunton & Pierce 2000:249; Hall, Herron, Pierce & Witt 2001:169; Hall, Herron & Pierce 2006:27; Hall *et al* 2012:127). These studies have indicated, amongst others, that the items selected were biased towards the ease of locating the item, the item's size, and the brightness of its colour. The presence of selection bias adversely impacts the randomness of the items selected, and could therefore lead to an unrepresentative and thus biased sample (and audit outcome). The use of a haphazard sampling technique is therefore not appropriate when used in conjunction with the application of statistical sampling techniques.

Block sampling is an alternative non-statistical sampling technique. This process requires the internal auditor to consciously focus on specific areas or blocks of data within an audit population, for example, a specific month or a specific payroll category within a payroll file (Apostolou 2004:19). The International Standards on Auditing (ISA) that addresses audit sampling (ISA 530) regards block sampling as an appropriate test procedure, but dismisses its use as an appropriate sampling technique. This dismissal is most probably due to this technique's limitations when internal audit is required to draw valid inferences about an audit population (Marx, Van der Watt & Bourne 2011:11-8).

3.3 Audit sampling pitfalls

Each sampling technique provides the internal auditor with advantages as well as presenting them with potential pitfalls. Therefore, all sampling techniques should be applied with caution. As mentioned previously, the choice of sampling techniques has a direct impact on the audit opinion regarding the effectiveness of governance, risk management and control processes. The internal auditor should therefore ensure that the processes of application, documentation and evaluation of the sampling technique used are conducted in a manner that will lead to reliable audit opinions. The most common pitfalls that internal auditors encounter with the use of sampling arise from the selection of the sample, and to a lesser extent, from the documentation and evaluation of the sample (Sumners 2008:169; Moeller 2009:204; Wortmann 2009; Hall *et al* 2012:127). The pitfalls relating to each of these phases are briefly listed below (Hall *et al* 2000:249; 2001:169; 2006:27; 2012:127). Although this is not a complete list, these pitfalls are the ones most commonly referred to in the literature.

In the first instance pitfalls regarding the selection of a sample include the use of a non-statistical technique, such as haphazard sampling (on the assumption that this is a viable alternative to a statistical sampling technique); selection of a non-representative sample (e.g. selecting a sample of the 20 largest branches from a population of 200 branches); the rationale underlying the sample selection is not clear; replacing sample items that could not be located from the original sample selection, and use of sample sizes that are too small to enable a valid inference to be drawn.

In the second instance pitfalls regarding the documentation of the sample include: omitting the sample size, the sample period and the description of the sample items; inaccuracies in recording the sample selection method and the details of the population. In the third instance pitfalls regarding the evaluation of the sample include situations where the implications of the analysis of the sample are not stated (i.e. are the results pertinent to the sample only, or are they representative of the population; and what impact does the results of the analysis of the sample have for the financial, regulatory and operational aspects of a company?); and, where a non-statistical sampling technique has been used, the sample results are assumed to be applicable to the population.

3.4 Mitigating strategies

A thorough search of the literature revealed that very little information is available on the mitigating strategies that internal auditors can implement to minimise the risks associated with audit sampling techniques while conducting an internal audit engagement. The IIA *Standards* do mention mitigating strategies in general when performing an internal audit engagement: internal auditors should have adequate knowledge and skills when conducting an engagement (IIA 2012:S1210; 2012:PA 1210-1); that policies and procedures should be developed to guide internal auditors in executing their duties, and that these may include working paper templates (IIA 2012:S2040; IIA 2012:PA2040-1); that engagements must be properly supervised, *inter* alia, to enhance the quality of the outcome (IIA 2012:S2340; IIA 2012:PA2340-1), and that a quality assurance and improvement assessment should be conducted both internally and externally (such as a peer review) to assess the efficiency and effectiveness of the activities of the internal audit function (IIA 2012:S1300). The inference is that these should also be appropriate for the application of sampling techniques. Although no specific indication is provided in the guidance on the evaluation of sampling techniques, ISA 610 (IFAC 2012b:ISA610) suggests that one of the aspects that should be examined by the external auditor before relying on the work performed by the internal auditors, is whether sufficient and reliable evidence has been obtained during the execution of an internal audit engagement. Similarly, nothing in the guidance suggests or requires that the audit committee should evaluate the sampling techniques used. However, as the audit committee is the overseer of internal auditing (IIA 2012:S2060; IOD 2009:93), it is a reasonable expectation that sampling techniques are also clarified (and sanctioned) by the overseeing body, if not for every internal audit engagement, then as part of the overall policies and procedures manual of the internal audit function. These seven mitigating strategies are further investigated in the empirical research conducted to identify the mitigating strategies implemented by the banking industry in South Africa.

4 RESULTS OF THE RESEARCH

The CAE, as head of the internal audit function, has a duty to ensure that the sampling technique used is the most effective one to mitigate the risks associated with sampling, thus improving the reliability of the internal auditor's opinion. The mitigating strategies preferred by the respondents to this study are provided in this section. As part of the process of ensuring that the research information obtained was of a high quality, background information was obtained on the professional standings of the participating CAEs. The results revealed that the heads of the locally controlled banks' internal audit functions were highly qualified: there were five chartered accountants (CA); one certified internal auditor (CIA); one certified information systems auditor (CISA); one MSc degree in Financial Engineering, and one respondent did not indicate his/her professional or educational credentials. In addition, the respondents indicated that they had between five and 22 years of experience in the routine selection and evaluation of audit sampling techniques. To further endorse the quality of the data, respondents were asked whether internal audit programs (referring to the detailed plan of the internal audit engagement) are reviewed and approved prior to the commencement of fieldwork. This process should enhance the reliability of the results derived from the intended test procedures. All the responding CAEs indicated that when conducting tests of controls the audit programs are reviewed and approved prior to the commencement of fieldwork. This practice ensures that the test procedures and the sampling technique to be employed are aligned with the test and audit objectives at the start of an internal audit engagement. Equally important is the fact that all the internal audit functions make use of formal or published guidelines on audit sampling techniques. This ensures that the application of the respective sampling techniques is aligned with the best practice guidelines, a situation which should also confirm the quality of the sampling techniques employed. Table 1 illustrates the most frequently referred to sources of guidance.

Table 1: Sampling guidance

Source/s of guidance	Response
The IIA's Practice Advisory 2320-3 on Audit Sampling	88.9% ranked this as the most or second most frequently referred to source
The International Standard on Audit Sampling (ISA530)	77.8% ranked this as either their first, second or third most frequently referred to source
Other*	44.4% identified these sources as their first or third most frequently referred to sources

*The banks' external auditor's requirements and documented sampling methodology.

From the above results, the two most frequently used sources are both authoritative international audit guidelines, namely the IIA's guidelines (88.9%) and the International Federation of Accountants (IFAC) guidelines (77.8%).

Questions were formulated to obtain information regarding the specific mitigating strategies implemented by the respondents to decrease the risks associated with sampling techniques. The questions posed were formulated in such a manner that the various elements of employing a sampling technique, namely a sample size, a sample selection and the evaluation of the sample results, were explored. In Table 2 these are respectively indicated as "a", "b" and "c" for each mitigating strategy explored.

The results revealed that 88.9% of the internal audit functions have mitigating strategies in place, designed to ensure the consistent application of sampling techniques. Seven specific mitigating strategies (refer to Table 2 number 1 to 7) and each activity's implementation to address the three sampling technique elements (indicated as "a", "b" and "c") are summarised below.

Respondents indicated that the preferred mitigating strategies are: the existence of the appropriate methodology (no.1); sign-off by supervisors (no.2); internal training provided (no.4), and the external auditor's evaluation (no.7). Respondents indicated that mitigating activities number 3 (peer reviews) and number 6 (evaluation by audit committee) enjoyed low implementation rates. A further observation is that for a specific mitigating activity the three elements of a sampling technique, namely sample size, sample selection and the evaluation of the sample results, were consistently rated either high or low except for mitigating activity number 5 (guidance templates) which obtained a high response rate for element "a", medium response rate for element "b" and a low response rate for element "c".

The main mitigating strategies being implemented by the respondents' internal audit functions include the following:

- Internal training on the application of the agreed internal audit methodology and sampling approach on both the sample size and the sample selection method (88.9%);
- Internally developed audit methodology which includes a sampling guideline applicable to both the sample size and the sample selection methods (88.9%);
- Sign-off by a superior or superiors within the audit department after the evaluation of the sample results (88.9%);
- Internally developed audit methodology which includes a guideline on the evaluation of sample results (77.8%);
- Sign-off by a superior or superiors within the audit department on both the sample size and the sample selection method (77.8%);
- Evaluation by the external auditors of both the sample size and the evaluation of the sample results (77.8%);
- Internal training on the application of the agreed internal audit methodology and sampling approach for the evaluation of sample results (66.7%);
- Evaluation of the sample selection method by the external auditors (66.7%); and
- Use of templates that guide the internal audit staff on the correct and consistent determination of appropriate sample size (66.7%).

Table 2: Mitigating strategies implemented

Variable	N	Yes	Mean	Std Dev
1a) Internally developed audit methodology which includes a sampling guideline on: Sample size	9	8	0.89	0.33
1b) Internally developed audit methodology which includes a sampling guideline on: Sample selection method	9	8	0.89	0.33
1c) Internally developed audit methodology which includes a sampling guideline on: Evaluation of sample results	9	7	0.78	0.44
2a) Sign-off by a superior/ superiors within the audit department on: Sample size	9	7	0.78	0.44
2b) Sign-off by a superior/ superiors within the audit department on: Sample selection method	9	7	0.78	0.44
2c) Sign-off by a superior/ superiors within the audit department on: Evaluation of sample results	9	8	0.89	0.33
3a) Evaluation through external peer reviews on: Sample size	9	2	0.22	0.44
3b) Evaluation through external peer reviews on: Sample selection method	9	2	0.22	0.44
3c) Evaluation through external peer reviews on: Evaluation of sample results	9	3	0.33	0.50
4a) Internal training on the use and application of the agreed internal audit methodology and sampling approach on: Sample size	9	8	0.89	0.33
4b) Internal training on the use and application of the agreed internal audit methodology and sampling approach on: Sample selection method	9	8	0.89	0.33
4c) Internal training on the use and application of the agreed internal audit methodology and sampling approach on: Evaluation of sample results	9	6	0.67	0.50
5a) Templates that guide the internal audit staff on the correct and consistent application of: Sample size	9	6	0.67	0.50
5b) Templates that guide the internal audit staff on the correct and consistent application of: Sample selection method	9	4	0.44	0.53
5c) Templates that guide the internal audit staff on the correct and consistent application of: Evaluation of sample results	9	2	0.22	0.44
6a) Evaluation by the audit committee on: Sample size	9	1	0.11	0.33
6b) Evaluation by the audit committee on: Sample selection method	9	1	0.11	0.33
6c) Evaluation by the audit committee on: Evaluation of sample results	9	2	0.22	0.44
7a) Evaluation by the external auditors on: Sample size	9	7	0.78	0.44
7b) Evaluation by the external auditors on: Sample selection method	9	6	0.67	0.50
7c) Evaluation by the external auditors on: Evaluation of sample results	9	7	0.78	0.44

These mitigating strategies should contribute positively to the quality and reliability of the results derived from the sample. Accordingly, the audit opinions that are derived from these results should also be reliable.

5 CONCLUSION

Within the South African banking industry there are many stakeholders that place reliance on the internal audit function's opinion on governance, risk management and control processes. These include the Supervisor, and the banks' boards of directors, audit committees, senior management teams, and external auditors. It is therefore vital that internal auditing's opinion is reliable. However, the reliability and integrity of the internal audit function's opinion may be called into question if an incorrect sampling technique is followed, one which might not be aligned with the audit and/or test objectives, or is technically inappropriate for the audit task. Mitigating strategies should be implemented by the CAE to improve the reliability and integrity of the internal audit opinion.

To confirm that the quality of information obtained during the empirical research on the mitigating strategies implemented within respondents' internal audit functions, the respondents' professional qualifications, years of experience, use of approved audit programs and reference to formal and/or published guidelines were explored.

It appears that the internal audit functions of the locally controlled South African banks implement the majority of the mitigating strategies intended to minimise the risks associated with sampling techniques, namely sampling risk, sampling bias and other pitfalls. For four of the seven mitigating strategies respondents indicated a high implementation rate (above 67%). These mitigating strategies are mostly linked to in-house interventions, namely the development of an appropriate methodology, supervision and training. The evaluation by the external auditors, an external mitigating activity, also recorded a high implementation rate. The only in-house intervention that received mixed responses was the development of templates as guidance to perform sampling techniques. Mitigating strategies focusing on the evaluation performed by external peer reviewers, as well as the audit committee, showed a low implementation rate. It is recommended that heads of internal auditing should explore implementing both these mitigating strategies because of the reliance that is placed on this opinion by the Supervisor, boards of directors, audit committees, senior management teams, and other stakeholders, which in turn highlights the importance of the function within this business sector (South Africa 2007, sect. 48 (v)(i); IOD 2009:95-100; Rezaee 2010:50; BIS 2012: 15; PwC 2012:18).

It is therefore important that the heads of the in-house internal auditing departments of the locally controlled banks continue to implement and extend the use of mitigating strategies or techniques in order to ensure the chosen sampling techniques result in reliable audit opinions.

REFERENCES

Aghili, S. 2011. Sampling Techniques. *The Internal Auditor,* December:19-21.

Alkafaji, Y., Hussain, S., Khallaf, A. & Munir, A.M. 2010. *Characteristics of an Internal Audit Activity (Report 1).* Institute of Internal Auditors Research Foundation. Altamonte Springs. Florida.

Apostolou, B. 2004. *Sampling: A Guide for Internal Auditors.* Altamonte Springs. Florida. The Institute of Internal Auditors Research Foundation.

Bank for International Settlements. 2012. *The internal audit function in banks.* [Online]. http://www.bis.org/publ/bcbs223.pdf (Accessed 16 July 2012).

Coetzee, P., Fourie, H. & Burnaby, P. Not dated. The internal audit profession in South Africa is growing faster than other regions: fact or fiction? Draft article submitted to the *Managerial Auditing Journal*. [E-mail to:] Smidt, L.A. (smidtla@tut.ac.za). 10 November 2014.

Crous, C., Lamprecht, J., Eilifsen, A., Messier, W., Glover, S. & Douglas, P. 2012. *Auditing and Assurance Services.* Berkshire: McGraw-Hill.

Dickie, D. (don.dickie11@yahoo.ca). 2014. Discussion with expert on statistics. [E-mail to:] Smidt, L.A. (smidtla@tut.ac.za). 24 November 2014.

Hall, T.W., Hunton, J.E. & Pierce, B.J. 2000. The use of and selection biases associated with non-statistical sampling in auditing. *Behavioral Research in Accounting*, 12:231-255.

Hall, T.W., Herron, T.W. & Pierce, B.J. 2006. How reliable is Haphazard sampling? *CPA Journal*, 76(1):26-27.

Hall, T.W., Higson, A.W., Pierce, B.J., Price, K.H. & Skousen, C.J. 2012. Haphazard Sampling: Selection biases induced by control listing properties and the estimation consequences of these biases. *Behavioral Research in Accounting*, 24(2):101-132.

Hall, T.W., Herron, T.L., Pierce, B.J. & Witt, T.J. 2001. Research notes; the effectiveness of increasing sample size to mitigate the influence of population characteristics in haphazard sampling. *Auditing: A Journal of Practice & Theory*, 20(1):169-185.

Hitzig, B.N. 2004. Statistical Sampling Revisited. *The CPA Journal*, 74(5):30-35.

Institute of Directors. 2009. *King Report on Governance for South Africa 2009.* South Africa. Institute of Directors in Southern Africa.

International Federation of Accountants (IFAC). 2012a. *International Standard on Auditing 530: Audit Sampling.* [Online]. http://www.ifac.org/sites/default/files/downloads/a027-2010-iaasb-handbook-isa-530.pdf (Accessed 9 January 2013).

International Federation of Accountants (IFAC). 2012b. *International Standard on Auditing 610: Using the Work of Internal Auditors.* [Online] Available from: http://www.ifac.org/sites/default/files/downloads/a027-2010-iaasb-handbook-isa-610.pdf [Accessed 24 April 2012].

Institute of Internal Auditors. 2012. *International Standards for the Professional Practice of Internal Auditing.* [Online]. https://global.theiia.org/ standards-guidance/Public%20Documents/IPPF%20Standards%20Markup%20Changes%202013-01%20vs%202011-01.pdf (Accessed 8 November 2012).

Institute of Internal Auditors. 2013. *Practice Advisories.* [Online]. https://global.theiia.org/standards-guidance/Member%20Documents/PAs_in_full.pdf (Accessed 31 May 2013).

Leedy, P.D. & Ormrod, J.E. 2005. *Practical Research-planning and design.* 8th ed. New Jersey: Pearson Prentice Hall.

Maingot, M. & Quon, K.T. 2009. Sampling Practices of Internal Auditors at Corporations on the Standard & Poor's Toronto Stock Exchange Composite Index. *Accounting Practice*, 8(3):215-234.

Marx, B., Van der Watt, A. & Bourne, P. 2011. *Dynamic Auditing.* 10th edition. South Africa: LexisNexis.

Moeller, R. 2009. *Brink's Modern Internal Auditing – A Common Body of Knowledge.* 7th edition. Canada, John Wiley & Sons.

PricewaterhouseCoopers (PwC). 2012. *Governance of Risk.* [Online]. http://www.pwc.co.za/en_ZA/za/assets/pdf/governance-of-risk.pdf (Accessed 22 January 2013).

Rezaee, Z. 2010. The importance of internal audit opinions. *The Internal Auditor,* 67(2):47-50.

South Africa. 2007. Banks Act, No. 20 of 2007. Government Gazette, 509(30474):1-60. [Online]. http://www.info.gov.za/view/Download FileAction?id=113033 (Accessed 19 April 2012).

Stuart, I.C. 2012. *Auditing and Assurance Services – An applied approach.* New York: Mcgraw-Hill.

Sumners, G.E. 2008. *CIA Exam review: Part II.* Baton Rouge: Sumners Audit Services.

Wortmann, R.E. 2009. Auditors: Use a clear sample. *Pensylvania CPA Journal*, Spring 2009. [Online]. http://www.picpa.org/Content/40012.aspx (Accessed 10 May 2013).

ANNEXURE A

The 10 locally controlled banks, in alphabetical order, are:

- African Bank
- Bidvest
- Capitec
- First Rand Bank
- Grindrod
- Investec
- Nedbank
- Sasfin
- Standard Bank
- UBANK

The performance audit: Are there differences in the planning approach and practices followed within the South African public sector?

E Gildenhuis
Department of Auditing
University of Pretoria

M Roos
Faculty of Military Sciences
University of Stellenbosch

ABSTRACT

The importance of a formal, documented approach and methodology as part of the audit process is well-recognised. In South Africa, only a few national departments have dedicated performance audit sections within the Internal Audit Function (IAF), and limited performance audits are being conducted. The limited execution of performance audits and the lack of information on performance audit methodologies adopted within the public sector by IAFs prompted this research. The research objective was to identify the differences in the performance audit planning practices followed by internal auditors within the South African public sector, as well as the reasons behind these differences, by critically comparing the performance audit methodologies within the IAFs in selected national departments with the methodology followed by the AGSA. The results indicated that, although differences do exist between the performance audit planning practices of these institutions and those of the AGSA, numerous similarities also exist. Research on the different planning activities prescribed by the methodologies adopted by national departments and the AGSA provides valuable information that may contribute to the growth of the performance audit discipline in the public sector and could enable the performance audit process itself to become more effective and efficient. It is recommended that national departments and the AGSA consider these differences and the rationale behind these differences when compiling or updating their performance audit methodology.

Key words

Performance audit; economy; efficiency; effectiveness; planning phase; Auditor-General; public sector; internal audit

1 INTRODUCTION

This article evaluates the requirement for, and evolution of, the *performance audit*[1] audit principle. This audit discipline came into being in response to the pressure placed on public sector entities by the increasing demand for their limited resources, along with the requisites to evaluate how these are utilised, to measure performance, and to ensure accountability (Jacobs 1998; Fakie 1999; Witthoft 1999; Ferdousi 2012; Loots 1989). There was an observable need for an audit discipline to be established (extending beyond financial auditing and financial management), in order to improve accountability and efficiency (De Jager 1999; Roos 1999; Al Athmay 2008).

The implementation of the performance audit discipline in South Africa at the Auditor General of South Africa (AGSA) is still relatively new, compared to traditional ‘regularity’ or ‘external’ auditing. Anecdotal evidence and personal experience in the field indicates that performance auditing within national departments in South Africa is still in its infancy. Only a few national departments have dedicated performance audit sections within their Internal Audit Functions (IAFs) and only a limited number of performance audits are being conducted. Although the performance audit is still a relatively new audit discipline at the AGSA, the performance audit methodology is well established and documented. The lack of information on performance audit methodologies adopted within the public sector by IAFs prompted this research. Initial analyses indicated differences between the performance audit methodologies adopted within the public sector and those followed by the AGSA.

Performance audits are required to determine whether stakeholders are getting value for money from the public sector (Guthrie & Parker 1999); if public funds can be better expended (Goolsarran 2007); and whether the right actions and activities are being undertaken by this sector. In addition, performance audits assess if these actions and activities are being undertaken correctly and efficaciously (Bi 2011), and whether service delivery is being conducted in the most economic, effective and efficient manner possible (Guthrie & Parker 1999; Al Athmay 2008; Reichborn-Kjennerud & Johnsen 2011; Van der Knaap 2011). Research on the differences in methodologies adopted by national departments, in comparison with the methodology followed by the AGSA, could provide valuable information which may contribute to the growth of the performance audit discipline in South Africa, and could enable the performance audit process itself to become more effective and efficient.

The mandate of the performance audit was originally established by the Supreme Audit Institutions, with the United States of America being the first to embrace this type of auditing in 1921. The USA was followed by Austria in 1948 and France in 1967. In 1974 the performance audit discipline was internationally accepted, with South Africa implementing the discipline in 1975, the Netherlands in 1976 (Pretorius & Botha 2013/14), Australia in 1976 (McCrae & Vada 1997), Canada in 1977, and the United Kingdom in 1983 (Pretorius & Botha 2013/14). Although the performance audit discipline was accepted by the AGSA in 1975, with the principles of the performance audit being incorporated into the Exchequer and Audit Act of 1975, it was only formally adopted and implemented in 1986, when the first performance audit was undertaken in the Department of Education and Training by the AGSA (Kluever 1999; Roos 2009). In 1987, Dr JH de Loor, the then Auditor-General of South Africa, indicated that the move towards implementing performance auditing by Supreme Audit Institutions was one of the most significant transformations in the roles and responsibilities of auditors, and would be the most value-adding support these state auditors could provide to the public sector (De Loor 1999).

2 RESEARCH OBJECTIVES

This research article aims to identify the differences in the performance audit planning practices followed by internal auditors within the South African public sector (as well as the reasons behind these differences), by critically comparing the performance audit methodologies within the IAFs in selected national departments with the methodology followed by the AGSA.

The key research question centres on determining whether there are differences between the performance audit planning practices of the AGSA and those of the IAFs currently conducting performance audits in selected national departments. If differences are identified, what are these differences and what is the reasoning behind the different approaches and practices?

3 METHODOLOGICAL FRAMEWORK

Research is described as

"[the] process of critical analysis to solve a problem. *Research has three important components:*
- *Critical knowledge enquiry.*
- *Discovery of new knowledge.*
- *Implementation and application of new knowledge."* (Lategan, Uwah & Swanepoel, 2011).

Firstly, with reference to the "*critical knowledge enquiry*" component, a detailed literature study was conducted to determine the meaning and mandate for performance auditing and the audit approach this requires.

As this study only focused on the performance audit within the public sector of South Africa, it was possible to obtain the performance audit methodologies of the AGSA and two national departments through formal approval processes. The advantages of multiple case study research include that it improves theory-building and, by comparing two or more cases, the researcher is able to establish the circumstances in which a theory will or will not be upheld (Bryman 2004). Both of the national departments selected for this study have fully implemented in-house internal audit units, each with a performance audit function and a formally implemented performance audit methodology.

In order to identify the differences between performance audit planning practices, a comparative analysis was conducted between the performance audit methodologies of the AGSA and the two selected national departments. The comparative analysis method aims to identify the similarities and differences between the methodologies implemented (Mouton 2001). The comparative analysis was informed by the utilisation of an assessment tool developed using the performance audit methodology of the AGSA as its baseline. Peer revision was sought from experts in the field to ensure the robustness and completeness of the assessment tool. Although the performance audit process consists of planning, fieldwork, and reporting phases, the assessment tool focused only on the planning phase. The fieldwork phase was specifically excluded from this research study due to the generic nature of the activities constituting this phase. The reporting phase, along with recent developments in the performance audit arena, will be addressed in a forthcoming article. The assessment tool was successfully utilised to review the performance audit methodologies of the national departments and the results were analysed to identify the differences. Follow-up interviews were conducted with senior managers responsible for performance auditing within the AGSA and in Department B, and with a director responsible for performance auditing within Department A, to identify reasons for differences and to validate the information obtained from the assessment tool, and the results.

As the performance audit discipline is still in an evolutionary phase within national departments, the results of the research could be utilised to enhance their respective methodologies. The AGSA could also use the information as part of their continuous assessment and improvement of the performance audit methodology they use and advocate. IAFs within national departments that have not yet instituted the performance audit discipline, or are in the process of instituting this mechanism, can utilise the results of the research in the compilation of a performance audit methodology. Utilising others' experiences and drawing from lessons others have learnt could expedite the growth of the performance audit discipline, ensuring greater efficacy and efficiency in its processes and activities.

4 LITERATURE REVIEW

The research focuses on identifying the differences between the performance audit methodology followed by the AGSA and those of the IAFs in the selected national departments. To be able to answer the research question it is necessary to analyse what is meant by *performance audit*, along with the methodology employed in pursuit of this phenomenon, and to investigate its development and implementation. This literature review describes the meaning and mandate for performance auditing, and the audit approach thereof.

4.1 Description and mandate for the performance audit

The International Organization of Supreme Audit Institutions (INTOSAI)[2] defines the performance audit (in the International Standard 300 of SAI), as "an independent, objective and reliable examination of whether government undertakings, systems, operations, programmes, activities or organisations are operating in accordance with the principles of economy, efficiency and effectiveness and whether there is room for improvement" (International Organization of Supreme Audit Institutions 2013). The definition provided by The South African Institute of Chartered Accountants (SAICA) extends the reference to 'room for improvement' made by INTOSAI by indicating that the performance audit should include a confirmation that appropriate managerial measures have been implemented to achieve the desired improvement (SAICA 2006).

Performance audit results should be conveyed in a detailed report to management, Parliament and other legislative stakeholders, should identify inadequate or non-existent managerial measures, and should include areas for improvement, as well as the corrective measures that will enable the public sector entity to improve its operations and control environment (Fakie 1999; Kluever 1999; Barret 2012). Ultimately, the result of a performance audit should "act as a catalyst for change" (Lourens 1999), through contributing to the improvement of public sector management, information, and accountability (Witthoft 1999).

The mandate for the performance audit in the South African public sector is strongly supported in legislation and guidelines, through the inclusion of the principles of performance auditing, viz., economy, efficiency and effectiveness (SAICA 2006; Prinsloo & Roos 2010). The Constitution of the Republic of South Africa (Section 195), identifies as one of the principles of public administration the fact that the "efficient, economic and effective use of resources must be promoted" Sections 38(1)(a)(i) and 51(1)(a)(i) of the Public Finance Management Act (National Treasury 2010) require the accounting officer of a department, trading entity, or constitutional entity, or the accounting authority of a public entity, to ensure that it "maintains effective, efficient and transparent systems of financial and risk management and internal control". Section 20(3) of the Public Audit Act (The Presidency 2005) indicates that the "Auditor-General may report on whether the auditee's resources were procured economically and utilised efficiently and effectively." Batho Pele, the White Paper on transforming public service delivery, includes as one of its eight service delivery principles "Value for money – public services should be provided economically and efficiently" (Department of Public Service and Administration 2007). The Batho Pele principle refers to the achievement of a cost effective public service through the identification of opportunities that will result in savings and an improvement in service delivery (National Treasury 2014).

The performance audit can be seen as a management tool (Ferdousi 2012) that focuses on current situations, circumstances and activities (Bi 2011) within a programme, activity or project (Ferdousi 2012), and aims to assist the organisation in improving future activities relative to the economical, efficient and effective procurement and use of its resources (De Loor 1999). The following section briefly summarises the purpose of a formal performance audit approach and methodology.

4.2 Performance audit approach

The analysis of the performance audit approach is considered a key element of the research process. Prior to this approach being discussed in detail, it is important to consider whether there is a difference between a performance audit conducted by external auditors (i.e. the AGSA) versus one undertaken by internal auditors (i.e. the in-house IAF of a national department). The regularity audit, also known as the financial audit or external audit, specifically focuses on financial statements, and accounting systems and procedures, together with compliance with legislation and financial standards (De Loor 1999). In contrast, the internal audit predominantly centres on improving the manner in which risks are managed and the value it will add to the organisation's operations (The Institute of Internal Auditors (IIA) 2012). However, the performance audit discipline, no matter by whom it is to be conducted, focuses on the principles of cost-effective and economical procurement of resources and the efficient and effective utilisation thereof (SAICA 2006; INTOSAI 2004). There should, therefore, be minimal differences between the manner in which and methodology by which the performance audit is conducted by the external auditors and the internal auditors.

The importance of a formal, documented approach and methodology as part of the audit process is well-recognised within the context of the performance audit; the purpose of a methodology[3] being to ensure that a structured and uniform approach is undertaken, ensuring the principles of performance auditing are maintained (SAICA 2006). The performance audit methodology should provide the performance auditor with sufficient guidance regarding audit selection, the audit approach, audit protocol, the reporting model to be used, and the process of quality assurance (Raaum & Campbell Jr 2006). Audit protocol should include, for example, the tools, techniques and studies to be utilised throughout all phases of the performance audit (Pollitt 2003); by what manner the managerial measures implemented by the entity should be evaluated; what means should be employed to obtain sufficient audit evidence; how this evidence should be analysed; and in what mode should value-adding recommendations be made (Jin'e & Dunkia 1997).

The performance auditor should be able to refer back to the methodology when an audit is being conducted; through this a uniform approach is ensured, while maintaining compliance with the guidelines and requirements of legislation and professional standards. However, the methodology should allow for flexibility in the design of a specific performance audit, as a performance audit is an individual undertaking, not a clear-cut 'one-size-fits-all' approach, and thus must allow for creativity and professional judgement (AFROSAI-e 2013). The Performance Audit Business Division, established at the AGSA, recognised early the importance of the process. They established guidelines in 1998, which included an approach to be followed during the planning, execution, reporting, and follow-up phases of a performance audit, as part of the first formal performance audit methodology (Pretorius 2014a; Kluever 1999; Lourens 1999).

Balkaran (2013) emphasises the importance of reviewing and updating audit methodology to ensure that the audit process incorporates all the latest technology and recent developments in the organisation and in the audit profession, as well as any amendments to legislation and standards with which compliance is required. The continual reviewing and updating of performance audit methodology is equally important because the performance audit discipline is a constantly developing, evolving and changing area (Independent Commission of Aid Impact 2011). The need for the review of and change to the performance audit methodology was also recognised by the AGSA and the performance audit methodology was amended in 1993, 1997, 2002, and 2007.

With the performance audit discipline within South Africa still in its infancy, regular reviews of and amendments to the methodology allow for any ineffective and inefficient processes to be amended (before becoming immovably embedded), and will thereby contribute to the performance audit becoming a value-adding, widely-accepted audit discipline performed in the most effective and efficient manner possible. Findings noted during the comparative analysis will be discussed in the subsequent section.

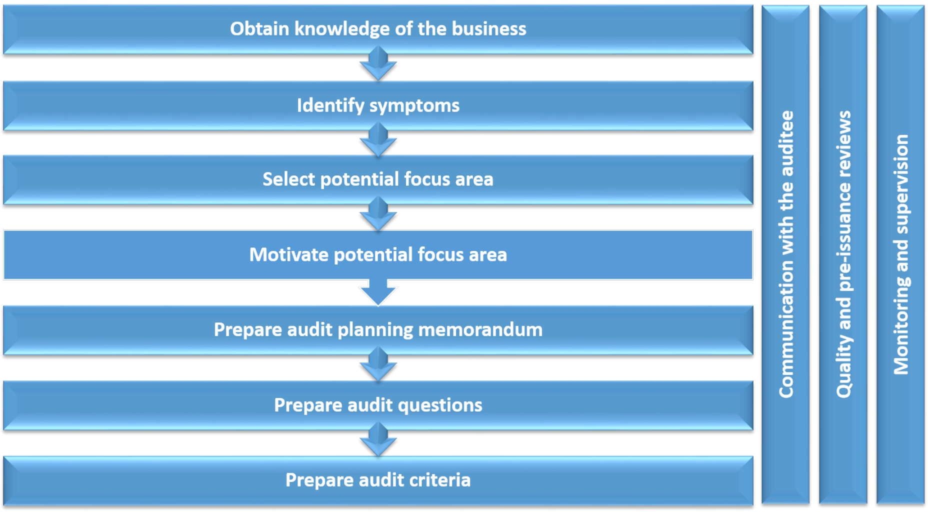
5 FINDINGS

As the methodology of the AGSA is utilised as a foundation for this analysis, a brief overview of the planning methodology is provided. The preparation and strategizing activities for a performance audit consist of a strategic planning process and the planning of individual performance audits.

The strategic planning activities concentrate on the identification and selection of performance audit focus areas where significant potential for weaknesses have been identified (AFROSAI-e 2013) and where the performance auditor will be able to add the most value when applying the principles of economy, efficiency and effectiveness. During this phase the AGSA takes into account the whole of the government to identify the principal focus areas and themes to be audited, including a focus area or theme specific to a government entity, or a transversal theme, which can be audited at more than one government entity.

The planning of individual performance audits will take into account the high level overview information obtained during the strategic planning phase, and will include a more detailed assessment of the selected focus area, to ultimately define the audit criteria against which the performance of the department, programme or project will be assessed (International Organization of Supreme Audit Institutions 2004). This assessment will also identify which specific aspects of the selected area are to be investigated in greater detail, in parallel with the sample of transactions or activities to be reviewed. The planning of individual performance audits consists of the following key activities:

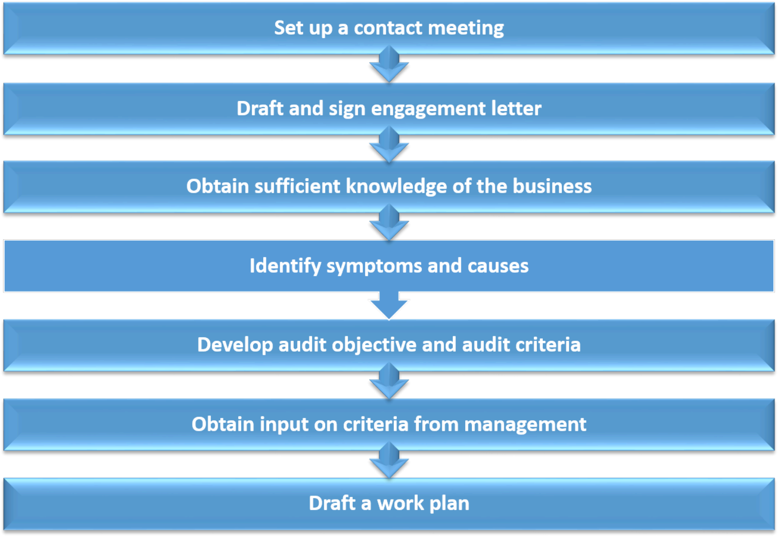
Figure 1: Outline of the AGSA planning phase


Obtain knowledge of the business
Identify symptoms
Select potential focus area
Motivate potential focus area
Prepare audit planning memorandum
Prepare audit questions
Prepare audit criteria
Communication with the auditee
Quality and pre-issuance reviews
Monitoring and supervision

Source: Performance audit manual of the Auditor-General of South Africa (2008)

As the methodology of the AGSA is utilised as a basis for comparison, it was considered necessary and prudent, for purposes of this study, to complete a high level comparison of the AGSA methodology with the other frequently used methodology in South Africa, that of Prinsloo & Roos (2010), as described in their book "Performance Auditing: A Step-by-Step Approach". The results of the high level comparison between AGSA and Prinsloo & Roos are discussed briefly as part of this section, after which the findings on the comparison between the AGSA and the IAF at national departments (being the primary objective of this article) are presented and discussed. Although the initial comparison of the planning methodology of the AGSA and Prinsloo & Roos revealed a number of differences, further investigation revealed that in essence the same methodology is recommended. The planning phase for individual audits as outlined by Prinsloo & Roos (2010) consists of the following activities:

Figure 2: Outline of the Prinsloo & Roos planning phase


Set up a contact meeting
Draft and sign engagement letter
Obtain sufficient knowledge of the business
Identify symptoms and causes
Develop audit objective and audit criteria
Obtain input on criteria from management
Draft a work plan

Source: Performance auditing: A step-by-step approach (Prinsloo & Roos 2010)

The major differences noted relate to the AGSA's requirements for communication with the auditee; selecting focus areas for the specific performance audit; performing quality and pre-issuance reviews; and lastly, monitoring and supervision throughout the audit. While the methodology of Prinsloo & Roos (2010) includes the setting up of a contact meeting, compiling the engagement letter, and obtaining inputs on the criteria from management as individual steps in the planning process, the AGSA groups these activities under the single requirement for continuous communication with the auditee. The AGSA requires selection of focus areas for the specific performance audit (i.e., sub-focus areas), which is not specifically addressed by the methodology of Prinsloo and Roos. Performing quality reviews, as well as monitoring and supervision throughout the audit, is not specifically covered by Prinsloo & Roos as part of their methodology, but these are covered in separate sections in the book. These differences are understandable in light of the methodologies having been developed in different contexts. The approach described by Prinsloo & Roos is more methodical and introductory and, as the title of the book suggests, provides "a step-by-step approach". The methodology described by the Auditor-General includes more information on the specific methods to be used during each of the different steps of the performance audit. The AGSA also needs to consider all the public sector departments and entities when selecting the focus areas during the strategic planning phase. It is therefore deemed reasonable that they would perform a more detailed assessment of the administration-wide focus areas selected during the strategic planning phase in order to decide on the focus or sub-focus areas for the individual performance audits. The AGSA planning methodology is considered to be a solid (comprehensive) basis for comparison with those of the IAFs in the selected national departments, and the results of this comparison are reflected below.

Comparing the key activities of the planning phase followed by the AGSA to the activities constituting the planning phase of the two national departments revealed certain variances. The table below highlights the differences noted, indicating whether or not the specific requirement was included or partially incorporated into the methodology of the national department. Although the table includes all the variances noted, due to space limitations for this article only those variances that might have the most significant impact on the performance audit methodology were selected for further discussion. With reference to the table below, the specific sections selected include: strategic planning (section 2); obtaining knowledge of the business (section 4.1); identifying symptoms (section 4.2); selecting the potential focus area (section 4.3); preparing the audit planning memorandum (section 4.5); quality and pre-issuance reviews (section 4.7), and monitoring and supervision (section 4.8).

Table 1: Comparison of key activities during planning phase

Requirement as per the methodology of the AGSA	Dept A	Dept B
1 Legislation, standards and guidelines		
Legislation, standards and guidelines to which the auditor needs to adhere during the planning phase have been explained.	✓	×
2 Strategic planning		
The methodology differentiates between strategic planning and the planning for the individual performance audits.	×	✓
The purpose of the strategic planning process is indicated as the process to facilitate the selection of performance audit focus areas.	n/a	✓
Formal selection criteria to be used when selecting focus areas are prescribed.	n/a	✓
The selection criteria include, *inter alia*, the following: (1) The value that can be added by conducting the performance audit; (2) Any problems or problem areas that have been identified; and (3) Any instances of risk or uncertainty that are inherent to that specific focus area. These focus areas can include aspects such as a significant budget and/or expenditure override; areas inclined to problems, such as procurement, new activities or changes in the environment; complex management structures and responsibilities; and the lack of accurate, complete, and reliable information.	n/a	⦸
The strategic planning process includes the following activities: (1) Obtaining an understanding of the potential focus area, which includes obtaining knowledge of the policies, strategies, budgets and operations of the focus area; (2) Monitoring the environment in which the focus area operates; (3) Continuous analysis of the performance audit areas; (4) Obtaining inputs from role players through a formal consultation process; (5) Preparing documentation to support and facilitate the approval to include the identified focus area in the annual performance audit coverage plan; (6) Maintaining proper methodology relating to the risk analysis and reporting; and (7) Identifying subject matter experts to be used during the proposed performance audit.	n/a	⦸
3 Annual coverage plan		
The methodology requires the department to compile an annual coverage plan indicating all the performance audits to be conducted during a specific financial year.	×	×
4 Planning of the individual audits		
The planning phase includes all of the following steps: (1) Obtain knowledge of the business; (2) Identify symptoms; (3) Select potential focus area; (4) Motivate potential audit focus area; (5) Prepare audit planning memorandum; (6) Prepare audit questions; (7) Prepare audit criteria; (8) Communication with the auditee (continuous); (9) Quality and pre-issuance reviews (continuous); and (10) Monitoring and supervision (continuous).	⦸	⦸
4.1 Obtaining knowledge of the business		
The process of obtaining knowledge of the business includes review and analysis of the following: (1) Legislation and relevant policies; (2) General programmes and performance goals; (3) Organisational structure and accountability relationships; (4) The objective, mission, and expected results; (5) Internal and external environment in which the entity operates, including major control systems and stakeholders; (6) External constraints affecting programme implementation; (7) Previous investigations and/or audits highlighting prior deficiencies or known problems; (8) Management processes and resources (including key personnel); and (9) Spending levels and revenues.	⦸	⦸
The methodology requires the auditor to document the knowledge of the business in a working paper.	×	×
4.2 Identifying symptoms		
The methodology describes the various approaches the auditor can utilise to identify symptoms, i.e. results-oriented approach or problem-oriented approach.	✓	×
The methodology requires the symptom identification to be properly documented and supported by sufficient evidence.	×	✓
The methodology requires that all symptoms are followed up and reasons to be provided should specific symptoms not be included in the final report.	⦸	×
4.3 Selecting a possible focus area		
The methodology indicates how possible focus areas will be identified and that the following criteria should be utilised when comparing the potential focus areas: (1) Performance targets are not being met; (2) Known problems exist; (3) Unauthorised over-expenditure or rising costs resulting in demands for more resources; (4) Fraud or other irregularities and deficiencies were indicated by previous audits or investigations; (5) A matter of special interest to Parliament, provincial legislature, or the public has been identified; (6) Internal control systems and evaluation are lacking; (7) Projects are not completed on time; (8) Delegations are abnormally limited or exceptional freedom is being allowed; (9) Inefficient, lengthy, obsolete, or useless procedures are being followed; (10) Unusual service conditions or fringe benefits are granted to personnel; (11) Complaints from staff or high staff turnover; (12) Misuse of machinery, equipment and other assets; and (13) The planning within the institution is weak.	⦸	×
4.4 Motivating a potential focus area		
The methodology requires the planning procedures be documented in a structured focus area memorandum.	⦸	×
The methodology requires the focus area memorandum to be approved by a delegated authority or committee.	✓	n/a
The methodology describes the layout and content of the focus area memorandum and includes the following: (1) Background information on the audited entity/function/programme/activity; (2) An evaluation of the risks identified, as formulated in the symptoms. (A detailed list of symptoms should be attached to the memorandum); (3) Materiality - which includes an assessment of the extent to which the symptoms or risks affect the service delivery objectives and the public; (4) Audit objectives and audit questions; (5) Proposed audit scope and a general description of the proposed audit approach; (6) Possible results of the audit and an indication of the contribution/impact the audit report will make; (7) Auditability with reference to the audit team's ability to carry out the audit in accordance with professional standards and audit policies; and (8) Recommendations.	×	n/a
4.5. Preparing an Audit Planning Memorandum		
The methodology requires that a detailed planning memorandum is compiled once the focus area has been approved and that this planning memorandum should include the following: (1) Audit problem/overall audit objective; (2) Final audit scope; (3) Audit questions; (4) Audit criteria; (5) Description of the audit approach and methodology; and (6) Resource planning, i.e. human resources, final cost & hours, timing of audit & preliminary report format.	×	×
The methodology requires that an appropriately delegated authority approve the planning memorandum.	n/a	n/a
The methodology requires any changes to the objective, scope, budget, cost, and timing of the audit to be resubmitted for approval by the same authority.	n/a	n/a
4.5.1 Audit problem/overall audit objective		
The methodology provides guidance on what defines an audit problem or audit objective.	×	×
4.5.2 Audit scope		
The methodology provides guidance on what defines the audit scope.	✓	×
The methodology requires that the audit scope be determined by asking *What*, *Who*, *When* & *Where*.	×	n/a

continued/

Requirement as per the methodology of the AGSA	Dept A	Dept B
4.5.3 Audit questions		
The methodology requires the auditor to compile detailed audit questions, broken down into specific and auditable sub-questions, once the scope has been determined.	×	×
4.5.4 Audit criteria		
The methodology provides guidance on what defines audit criteria.	✓	✓
The methodology indicates the following as potential sources of audit criteria: (1) Laws, regulations and other requirements governing the operations of the audited entity; (2) Decisions made by the legislature or the executive; (3) Standards developed by recognised professional organisations that follow due process; (4) Key performance indicators and performance standards set by the auditee or the government; (5) New or established scientific knowledge and other reliable information; (6) Criteria used previously in similar audits or by other SAIs; (7) Independent expert advice and know-how; (8) Organisations (local or foreign) carrying out similar activities or having similar programmes; and (9) General management and subject-matter literature.	⦸	×
The methodology requires the auditor to discuss the audit criteria with the auditee and to formally document evidence of such discussions.	⦸	×
4.5.5 Audit approach and methodology		
The methodology requires that the audit approach should be based on the audit objectives, scope, and criteria, and should include procedures that will determine the causes and effects of any findings noted.	⦸	×
The methodology indicates that the audit approach can include, *inter alia*, the following data-gathering techniques: (1) Surveys; (2) Interviews; (3) Observations; and (4) Desktop review of relevant documentation.	×	×
4.6 Communication with the auditee		
4.6.1 Contact meeting		
The methodology requires a contact meeting to be held with the project sponsor and senior officials before commencing with the audit.	✓	✓
The methodology requires that the following should be discussed during the contact meeting: (1) Details of the performance, for example the audit budget; (2) The principles of the performance audit; (3) The process that will be followed; (4) A request that the audit committee be informed of the pending audit; (5) Background of the business/ programme/ project/ activity being audited; (6) Establishment of a steering committee for the audit; (7) Appointing a contact person on behalf of the auditee; (8) Arrangements to introduce the audit team to the senior officials of the auditee; and (9) Logistical arrangements in terms of access to the building and office space.	⦸	⦸
4.6.2 Steering committee		
The methodology indicates that a steering committee should be formed for the audit and that the following individuals should form part of this committee: (1) The senior members of the audit team; and (2) Two senior officials from the auditee, one of whom should act as the Chairperson.	⦸	×
The methodology requires that detailed minutes of the steering committee meetings should be maintained.	O	n/a
4.6.3 Engagement letter		
The methodology explains the purpose of the engagement letter and requires that the engagement letter be sent to the auditee prior to the commencement of the engagement.	✓	✓
The methodology prescribes the layout of the engagement letter, which includes, *inter alia*, the following: (1) The mandate of the performance audit team; (2) The objective of the performance audit; (3) Management's responsibility regarding the implementation of management measures to ensure the economic, efficient and effective use of resources; (4) The scope of the audit, including reference to the applicable legislation and regulations; (5) The reporting structure or other means of communication of the results of the engagement; (6) Access to records and documentation required for the audit; and (7) Any other specific details regarding the audit.	×	⦸
4.7 Quality assurance and pre-issuance review		
The methodology requires that a detailed quality assurance review be conducted prior to the commencement of the execution phase.	⦸	⦸
The methodology requires the results of the quality assurance review to be formally documented in a working paper.	×	×
4.8 Monitoring and supervision		
The methodology requires that proper monitoring and supervision of the work performed by the audit team should be conducted to ensure that the audit objective is achieved.	×	×

Source: Performance audit manual of the Auditor-General of South Africa (2008)

Tick legend

✓	Requirement was addressed in the methodology of the national department.
×	Requirement was not addressed in the methodology of the national department.
⦸	Requirement was partially addressed in the methodology of the national department, either by only including some of the aspects, or by only incorporating the aspects as part of the templates included in the methodology.

Differences identified in Table 1, with specific reference to strategic planning, obtaining knowledge of the business, identifying symptoms, selecting the potential focus area, preparing the audit planning memorandum, quality and pre-issuance reviews, and monitoring and supervision, are further analysed and discussed in the following subsections.

5.1 Strategic planning

The AGSA utilises specific criteria (as indicated in Section 2 of Table 1) when identifying and selecting critical areas. Comparison of the selection criteria employed by the AGSA and Department B revealed certain distinctions. Additional selection criteria included by Department B are: public complaints; the potential for cost savings and service improvements; financial conditions; visibility of the programme or sub-programme; risk of loss, fraud or corruption; public welfare; management interest; legislative interest; public interest; recent audit coverage; new developments; and areas of non-performance identified during the audit of predetermined objectives.

5.2 Planning of individual performance audits

Initial consideration appears to indicate inconsistency and omission when comparing the different planning activities of the three entities. Further analysis reveals that the same activities are performed, although different terminology is used and some of the activities are consolidated with other steps as part of the planning process. To ensure a more detailed and comprehensive testing of consistency the different key activities incorporated in the planning process of the three entities were compared and the significant differences are reflected below.

5.3 Obtaining knowledge of the business

In the AGSA's methodology, obtaining knowledge of the business, as seen in Section 4.1 of Table 1, involves considering various aspects which, with the exception of legislation and relevant policies, refers to the information that can be obtained within documents and not the documentation itself. The methodology of Department A does not provide guidance on the specific aspects that should be considered when obtaining knowledge of the business, but provides an overview of the methods that should be used to obtain this knowledge, in consort with the documentation that should be reviewed. The methodology of Department B incorporates both aspects.

As noted in Table 1, the methodology of neither national department explicitly requires the auditors to document the results of obtaining knowledge of the business in a working paper; however, discussions with the director and senior manager responsible for performance auditing in the respective departments revealed that this information is documented. The auditors of Department A record this information in their symptom identification document (which is not mentioned in the methodology), and those of Department B detail this information as part of the record of symptoms and management measures, which is included as an annexure to the methodology. One of the departments' procedures included documented detailed process descriptions for the focus area that can then be used during future audits, although this is not specifically stated within the methodology.

5.3.1 Identifying Symptoms

The methodology of the AGSA indicates that the identification of symptoms should be performed via either the result-oriented or the problem-oriented approach. Similarly, the methodology of Department A refers to these two approaches; however the advocated methodology of Department B makes no reference to either. The senior manager responsible for performance auditing within Department B indicated that the reason no reference is made to the problem-orientated and results-orientated approaches is so the auditors are not constricted or limited to one specific method. Either approach may be employed in any performance audit performed by the department.

5.3.2 Selecting a potential focus area

When selecting the potential focus areas (sub focus areas) within the primary focus area identified during the strategic planning phase, the AGSA methodology prescribes the consideration of certain factors as part of the process to determine the sub-focus areas when evaluating the identified symptoms. Comparing the criteria used by Department A to select the potential focus areas of the individual performance audits to those prescribed by the methodology of the AGSA, as seen in Section 4.3 of Table 1, revealed numerous similarities: however, two aspects were excluded and four additional facets incorporated. The additional criteria encompassed in the matrix employed by Department A included: "no performance audit being carried out in the last three years"; "results of previous audits revealed various discrepancies"; "important services are rendered that are aligned to the strategic objectives of the department"; and "services provided by the department have been extended or new services have been added". The additional selection criteria are intended to ensure that all key services and activities of the department are subjected to a performance audit and all aspects which could be incorporated in a performance audit (for instance any risks or deficiencies identified during other types of audits), have been considered during the selection of the focus area.

5.3.3 Preparing an audit planning memorandum

The required planning memorandum in the methodology of the AGSA encompasses various aspects, including the audit objective, scope, questions, criteria, and approach and methodology. Although neither of the methodologies makes specific reference to a planning memorandum, some of these factors are addressed separately in the methodologies of the national departments, as reviewed below.

Only the Department A methodology supplies direction as to what defines the audit scope. The methodology of the AGSA indicates that the auditors should determine the scope by asking "*what, who, when and where*", while the methodology of Department A specifies that the scope be determined by considering the systems, records, personnel, and physical properties. The senior manager responsible for performance auditing within Department B did, however, mention that the template for the engagement letter, included as an annexure to the methodology, includes a section for the audit scope, and also provides guidance on what the scope should entail.

Although both methodologies provide direction as to what defines audit criteria, only the methodology of Department A indicates what can be utilised as criteria sources, and is in this regard similar in methodology to that of the AGSA. Comparing the sources of criteria outlined in the methodology of Department A to those prescribed by the methodology of the AGSA (as indicated in Section 4.5.4 of Table 1) revealed significant differences. The criteria sources indicated in the methodology of Department A exclude five of those prescribed by that of the AGSA. These encompass: decisions made by the legislature or the executive; new or established scientific knowledge and other reliable information; criteria used previously in similar audits or by other SAIs; independent expert advice and know-how; and general management and subject-specific literature. Additionally, the sources indicated in the methodology of the department incorporate one aspect not mentioned in the methodology of the AGSA, namely the historical performance of the department, division, or local institutions.

5.3.4 Quality assurance and pre-issuance review

The methodology of the AGSA incorporates a specific section indicating the requirements for quality assurance and pre-issuance review. However, both national departments' methodologies omit any reference to this. The director responsible for performance auditing within Department A indicated that aspects relating to the quality and pre-issuance reviews are addressed in the primary internal audit manual of the IAF. The methodology of Department A incorporates a quality assessment review checklist as an annexure to the methodology.

5.3.5 Monitoring and supervision

Similarly to the findings of the analysis on quality assurance and pre-issuance review requisites, the methodology of the AGSA incorporates a specific section indicating the requirements for monitoring and supervision during the planning phase of the performance audits. Although it is not specifically mentioned in either department's methodology, both individuals responsible for performance auditing indicated that monitoring and supervision is fundamental to the approach followed by the audit team.

6 DISCUSSION

The preceding analysis clearly demonstrates that there are differences between the performance audit methodologies of the AGSA and those of the national departments selected for this research. In the course of the analysis various themes and trends emerged providing possible explanations for the differences in the adopted methodologies. The most significant contributing factor to the differences in performance audit methodologies can be ascribed to the different objectives of the external audit (AGSA) versus the internal audit (within the two departments forming part of this research). An additional significant reason is that the performance audit methodology forms part of the primary internal audit methodology adopted within national departments, whereas it is a stand-alone methodology at the AGSA. Furthermore, the guidelines that inform which performance audit approach is to be adopted differ between the AGSA and the departmental IAFs. The departments incorporate templates of working papers that guide the performance auditors and provide additional information, as part of their methodology, whereas the methodology of the AGSA is explained in a performance audit manual that is without templates. Discussions also revealed that many activities and tasks are performed, although not specifically included or explicitly required in the formal documented performance audit methodology of the IAF. The above-mentioned contributing factors are discussed in more detail below.

The focus of both the external and IAFs is on economy, efficiency, and effectiveness as part of the performance audit process; however, the objectives, audience or users, reasons for conducting performance audits, and accountability structures differ. The AGSA performance auditors are external to the entity being audited, while the performance auditors employed in the IAFs of the national departments are seen as part of the organisation. The purpose of performance auditing within the AGSA is to facilitate improvements to public administration within the public sector, by providing parliament and government entities with value-adding recommendations, in consort with the provision of impartial and trustworthy information as to how these entities are performing, in order to promote public transparency and accountability (Auditor-General of South Africa 2014). The audience and users of the performance audit reports issued by the AGSA would therefore be the legislature and management of the entity being audited. Conversely, the purpose of the performance audit within the IAF is based on the principle of improvement, as it is their responsibility to add value and suggest improvements to the operations of the organisation (The Institute of Internal Auditors 2013).

The performance auditors form part of the IAFs of the national departments and need to comply with the prescriptions included in the overall Internal Audit Methodology. As a result, many activities included in the AGSA performance audit methodology form part of the overall Internal Audit methodology and are not duplicated in the performance audit methodology.

In addition, the detailed comparison revealed different approaches to strategic planning. The AGSA and one department include strategic planning as part of the overall planning process specific to the performance audit, while performance audit planning for the other department is incorporated into the formal planning for the IAF, with the detailed development of the performance audit only performed once the focus area has been selected.

Both national departments' methodologies include specific templates to be utilised by the performance auditors, whereas the methodology of the AGSA is not prescriptive in this regard. The AGSA has templates that are available on the electronic audit management system. Despite the existence and use of templates within the departments, however, it was noted that in certain instances the methodologies do not refer to them. The purpose of including the templates as part of the audit management system at Department B is to ensure compliance with the performance audit methodology requirements. The senior manager is of the opinion that general templates will make the audit process more efficient, but cautions against incorporating templates in the performance audit methodology as this may restrict the performance auditors when conducting the various tasks and activities, and reduce or negate innovative and original thinking (Pretorius 2014b).

An additional theme worth mentioning is that some activities prescribed by the methodology of the AGSA were not included in those of the national departments. The director and the senior manager responsible for performance auditing within these entities are of the opinion that these are activities and procedures any performance auditor should be aware of, or which are integral to the audit process.

7 CONCLUSION AND AREAS FOR FUTURE RESEARCH

The purpose of the research was to identify differences in the performance audit planning practices followed by internal auditors in the South African public sector. This was undertaken by critically comparing the audit methodologies within the IAFs in the selected national departments with that followed by the AGSA. When this study was commenced there were very few IAFs within the national departments that had formally adopted and implemented the performance audit discipline. As a result, the number of methodologies that could be utilised for purposes of this research was limited. The underlying reasons and causes for the limited implementation should therefore be investigated. An initial explanation could be the lack of readily available standards and guidelines on the methodology to be utilised by the IAF when performance audits are conducted.

Despite the limited number of methodologies utilised for the research, the analysis of the methodologies of the two national departments that were selected provided valuable information and insights. The results indicate that, although differences do exist between the performance audit planning practices of these institutions as compared to those of the AGSA, they also share numerous similarities. The basic building block of performance auditing (the identification of symptoms and the articulation of findings in accordance with the three ‘Es’ of economy, efficiency, and effectiveness), was present in all three methodologies. All three entities strive towards a similar outcome - that of adding value and improving performance within their unique environments, guided by the rules and practices of each specific organisation. By utilising the detailed results of the comparative study reflected in this article, other performance auditors can develop or enhance their performance audit methodologies.

A recurring theme throughout the results is that not all activities are specifically included as part of the performance audit methodology. The primary reasons appear to be that these are incorporated in the overall internal audit manual of the IAF, or in the templates of the working papers, or it is expected of performance auditors to conduct these activities whether or not they are specifically included in the formally documented performance audit methodology. The danger of not explicitly incorporating these activities as part of the methodology, or of failing to specifically refer to requirements contained in the primary internal audit manual, increases the potential for overlooking or omitting important principles and activities of performance auditing. In addition, to enable adequate quality control it is considered a requisite to have a complete, comprehensive baseline or control against which actual performance can be measured. Further research could thus be conducted to determine the extent of performance auditors’ awareness of the full spectrum of audit activities not specifically addressed as part of the methodology.

Overall, the results of this research could be valuable not only for the participants in this study but also for any other public sector entities considering implementing the performance audit discipline within their IAFs. Those with existing performance audit methodologies could gain from the experiences and lessons learnt in this article in order to update and improve their processes.

ENDNOTES

[1] A variety of terms for performance auditing have been utilised from its inception, with the two most common being value-for-money auditing (Kells & Hodge 2010; Lonsdale 2000) and operational auditing (Flesher & Zarzeski 2002). At the Twelfth International Congress of Supreme Audit Institutions in April 1986, however, the term performance auditing was formally accepted by all Supreme Audit Institutions (Witthoft 1999) and will be used for purposes of this article.

[2] INTOSAI is an international organization of the Supreme Audit Institutions from a significant number of nations that includes the National Audit Office of Australia; Office of the Comptroller and Auditor-General of Bangladesh; Office of the Auditor-General of Canada; National Audit Office of Denmark; The State Audit Office of the Estonia; The Ghana Audit Service; State Comptroller’s Office of Israel; Netherlands Court of Auditors; Office of the Auditor-General of Norway; The Philippine Commission on Audit; National Audit Office of Sweden; and the State Audit Office of Thailand, amongst others.

[3] The AFROSAI-e Performance Audit Manual dated November 2013 indicates the methodology should “*contain generally accepted guidance and good practice, and cover on a more detailed level performance auditing in different sectors, or certain methods to be used in the performance audit process*”.

REFERENCES

AFROSAI-e. 2013. *Performance Audit Handbook,* Unknown: AFROSAI-e.

Al Athmay, A-A.A.R.A. 2008. Performance Auditing and Public Sector Management in Brunei Darassalam. *International Journal of Public Sector Management*, 21(7):798-811.

Auditor-General of South Africa. 2008. *Performance Audit Manual.* Pretoria: Auditor-General of South Africa.

Auditor-General of South Africa. 2014. *Auditor-General of South Africa - Auditing to build public confidence.* [Online]. http://www.agsa.co.za/Auditinformation/Performanceauditing.aspx (Accessed 01 November 2014).

Balkaran, L. 2013. The Importance of an Audit Manual. *Internal Auditor*, 01 April.

Barret, P. 2012. Performance Auditing - Adressing Real or Perceived Expectation Gaps in the Public Sector. *Public Money & Management*, 32(2):129-136.

Bi, L. 2011. *ICGFM Conference.* Miami, The Institute of Internal Auditors.

Bryman, A. 2004. *Social Research Methods.* New York: Oxford University Press.

De Jager, H. 1999. Performance Auditor for the Private Sector? *Auditing SA*, Issue Jubilee Issue:42-43.

De Loor, D.J.H. 1999. Challenges Facing Supreme Audit Institutions. *Auditing SA*, Issue Jubilee:10-13.

Department of Public Service and Administration. 2007. Batho Pele Handbook: A Service Delivery Improvement Guide. [Online]. http://www.dpsa.gov.za/batho-pele/docs/BP_HB_optimised.pdf (Accessed 26 July 2014).

Fakie, S. 1999. Challenges for Performance Auditing. *Auditing SA*, Issue Jubilee Issue:8-9.

Ferdousi, N. 2012. *Challenges of Performance Audit in the Implementation Phase: Bangladesh Perspective,* Bangladesh: North South University.

Flesher, D.L. & Zarzeski, M.T. 2002. The Roots of Operational (value-for-money) Auditing in English-Speaking Nations. *Accounting and Business Research*, 32(2):93-104.

Goolsarran, S.A. 2007. The Evolving Role of Supreme Audit Institutions. *The Journal of Government Financial Management*, 56(3):29-32.

Guthrie, J.E. & Parker, L.D. 1999. A Quater of a Century of Performance Auditing in the Australian Federal Pubic Sector: A Malleable Masque. *ABACUS*, 35(3):302-332.

Independent Commission of Aid Impact. 2011. *ICAI's Approach to Effectiveness and Value for Money,* London: Crown.

International Organization of Supreme Audit Institutions. 2004. *ISSAI 3000: Standards and Guidelines for Performance Auditing based on INTOSAI's Auditing Standards and Practical Experience,* Copenhagen: INTOSAI Professional Standards Committee.

International Organization of Supreme Audit Institutions. 2013. *ISSAI 300: Fundamental Principles of Performance Auditing,* Copenhagen: INTOSAI Professional Standards Committee.

Jacobs, K. 1998. Value for Money Auditing in New Zealand: Competing for Control in the Public Sector. *British Accounting Review*, 30(4):343-360.

Jin'e, Y. & Dunkia, L. 1997. Performance Audit in the Service of Internal Audit. *Managerial Accounting Journal*, 12(4/5):192-195.

Kells, S. & Hodge, G. 2010. Redefingin the Performance Auditing Space. *Asia Pacidic Journal of Public Administration*, 32(1):63-88.

Kluever, H. 1999. Brief Overview on the History of Performance Auditing in the Office of the Auditor-General. *Auditing SA,* Issue Jubilee Issue:6-7.

Lategan, L.O.K., Uwah, Z. & Swanepoel, H. 2011. Doing Research: Navigating the Process. In Lategan, L.O.K., Lues, L. & Nel, H.F. (eds.) *Doing Research*, revised edition. Bloemfontein: Sun Press:1-5.

Lonsdale, J. 2000. Developments in Value-For-Money Audit Methods: Impacts and Implications. *International Review of Administrative Sciences*, 66(1):73-89.

Loots, J.A.J. 1989. An Evaluation of the Applicability of Comprehensive Auditing in the South African Context. D.Com(Acc) Thesis. University of Pretoria. Pretoria.

Lourens, G. 1999. Performance Auditing - Then and Now. *Auditing SA*, Issue Jubilee:24-26.

McCrae, M. & Vada, H. 1997. Performance Audit Scope and the Independence of the Australian Commonwealth Auditor-General. *Financial Accountability & Management*, 13(3):203-223.

Mouton, J. 2001. *How to Succeed in your Master's & Doctoral Studies - A South African Guide and Resource Book.* Sixteenth impression 2012 ed. Pretoria: Van Schaik .

National Treasury. 2010. *Public Finance Management Act No. 1 of 1999,* Cape Town: Goverment Gazette.

National Treasury. 2014. *National Treasury: Batho Pele Principles.* [Online]. http://oag.treasury.gov.za/RMF/Pages/s609BathoPelePrinciples.aspx (Accessed: 16 July 2014).

Pollitt, C. 2003. Performance Audit in Western Europe: Trends and Choices. *Critical Perspectives on Accounting*, 14(1-2):157-170.

Pretorius, C. 2014a. *History of Performance Audit at the Auditor-General of South Africa* [Interview] (15 July 2014).

Pretorius, C. 2014b. *Senior Manager: Performance Auditing* [Interview] (20 October 2014).

Pretorius, C. & Botha, C. 2013/14. A Short History of Performance Auditing in South Africa. *Auditing SA*, Issue Summer:27-30.

Prinsloo, J. & Roos, M. 2010. *Performance Auditing: A Step-by-Step Approach.* Second ed. Pretoria: Van Schaik Publishers.

Raaum, R. B. & Campbell Jr, R. 2006. *Challenges in Performance Auditing: How a State Auditor with Intriguing New Performance Auditing Authority is Meeting Them,* Alexandria: Association of Government Auditors: Corporate Partner Advisory Group.

Reichborn-Kjennerud, K. & Johnsen, A. 2011. Auditors' understanding of evidence: A performance audit of an urban development programme. *Evaluation*, 17(3):217-231.

Roos, M. 1999. Performance Auditing: Views of the Institute for Public Finance and Auditing. *Auditing SA*, Issue Jubilee Issue:44-45.

Roos, M. 2009. Performance Management within the Parameters of the PFMA M.Com Thesis. University of South Africa. Pretoria.

South Africa. 1996. *Constitution of the Republic of South Africa Act 108 of 1996,* Cape Town: Government Gazette.

The Institute of Internal Auditors. 2012. *International Standards for the Professional Practice (Standards),* Florida: The Institute of Internal Auditors.

The Institute of Internal Auditors, 2013. *The Institute of Internal Auditors.* [Online]. http://www.theiia.org/guidance/standards-and-guidance/ippf/definition-of-internal-auditing/?search%C2%BCdefinition
(Accessed 01 November 2014).

The Presidency. 2005. *Public Audit Act No. 25 of 2004*, Cape Town: Government Gazette.

The South African Institute of Chartered Accountants. 2006. *Guide on Performance Audit in the Public Sector,* Kengray: The South African Institute of Chartered Accountants.

Van der Knaap, P. 2011. Sense and Complexity: Initiatives in Responsive Performance Audits. *Evaluation*, 17(4):351-363.

Witthoft, G. 1999. Performance Auditing: 1987. *Auditing SA*, Issue Jubilee Issue`;14-19.

Quality of internal audit reports

S Mungal
Department of Auditing
University of Pretoria

J Slippers
Department of Business Management
University of Pretoria

ABSTRACT

The purpose of this paper is to explore the completeness and quality of audit reports as perceived by internal audit's primary customer – the audit committee.

Data was collected using a structured questionnaire that was sent to audit committee chairpersons of banks registered with the South African Reserve Bank. Respondents were asked to provide their perceptions of the quality of the internal audit reports they routinely received.

The results highlight that not all internal audit functions present clear and appropriately focused reports. Whilst the audit committee chairpersons recognise that the internal audit reports do have value, there is also significant potential for improvement.

Key words

Internal audit; report; communication; quality

1 INTRODUCTION

While an internal audit function's fieldwork could be of exceptional quality, unless the written audit report has a matching quality of insight and clarity of expression, it seldom meets stakeholder expectations; furthermore, the report could in fact negate the value internal audit strives to add to the business.

The International Standards for the Professional Practice of Internal Auditing (herein referred to as the Standards) require the internal audit function to report periodically to senior management and to the board on the nature and extent of the risks the organisation is exposed to, and on control issues, fraud exposures and governance issues (IIA 2012:14). The board delegates this role to the audit committee (AC) which is then required to report to the board on internal audit matters. (For the purposes of this research paper, the term internal audit function will be used interchangeably with internal auditing, as no significant distinction of meaning was apparent in the literature reviewed for this paper).

The internal audit function usually provides information to the AC through written audit reports (Schneider 2009:24). The internal audit report consists of factual findings which have been identified during the execution of the audit, and serves as the formal tool of communication to stakeholders on the state of governance, risk exposure and control functions of an organisation.

Rittenberg (2002:32) explains that ACs require an effective information-gathering and dissemination system which is comprehensive, objective and comprehensible in order for it to perform its duties effectively. Internal Audit can assist the AC with this information requirement by preparing an internal audit report that meets the aforementioned criteria.

Internal audit is recognised as being the eyes and ears of an AC, enabling the AC to provide independent feedback to the board (IIARF 2009:10). Thus, internal audit is in a favourable position to assist the AC in the effective discharge of its duty to report to the board.

A study conducted by PwC (2011:18) asserts that internal audit's "favourable position" is in fact a *unique* position as it is probably the only function that looks at every process across an organisation, and therefore has the unique ability to see the interconnectedness of processes and how they contribute to achieving the organisation's objectives.

Internal audit should therefore be using this position to their advantage and be pulling meaningful information (fraud, risk and governance exposures and control issues) from audits they have performed, incorporating this information into their reporting activities, and thus providing greater value and insight to the AC, thereby increasing the relevance of the internal audit function.

2 PURPOSE OF THE STUDY

The results of a recent survey conducted by PWC (2014:2) reveal that 30% of board members believe that internal audit adds less than "significant value" to organisations. As the deliverable emerging from every internal audit engagement is the internal audit report, the question that arises is whether the audit reports are fairly conveying the situation discovered during the audit: in other words, would this perception change if the contents and writing style of the audit reports provided to the AC were improved?

Sufficient literature exists to provide persuasive perspectives on the quality of the internal audit function as a whole (Cathcart & Kapoor 2010:48; IIA 2014:5; Kapoor & Brozzetti 2012:1; Plant & Steyn 2010:6). However only a limited number of studies have been performed on the quality of the internal audit reports issued to their primary customers - the AC.

The recent collapse of African Bank has been attributed to weaknesses in the bank's micro lending/ credit approval processes, weak governance structures and inappropriate regulatory oversight (Whitfield 2014:7). The question that arises from this is: why was the board unable to grasp the magnitude of the problems being experienced in African Bank *before* it was too late?

It is therefore relevant to explore the quality (completeness of content and clarity of writing) of reports that internal audit submits to AC chairpersons in South Africa's banking industry. For purposes of this research, the evidence collected to determine the quality of audit reports has been limited to the perceptions of chairpersons of ACs in South Africa's banking industry.

However, this introduces a limitation to the validity of this study in that the empirical research extends only to the views (perceptions) of AC chairpersons in the banking industry. Other limiting aspects were that no linguistic analyses were performed on the text of the reports the AC chairpersons had in mind when responding, nor were the findings verified by independent outside authorities. The results presented here should therefore not be seen as a generic view (applicable across all industries), of the value that internal audit reports add to the internal audit function's reputation. However the results do offer insights which other industries may find useful when reviewing their current reporting practices.

This research paper therefore focuses solely on the report presenting the internal audit function's audit engagement results to the AC chairperson. The primary objective of this research is to identify the current perceptions of the banking industry's AC chairpersons on the value of the content and accessibility of writing style of the internal audit reports they receive.

If poorly written internal audit reports, containing impractical or irrelevant information, are received by ACs, the AC chairpersons are unlikely to relay information on internal audit matters in any way that warrants the positive attention of the board. This then creates a negative impression of the value of the internal audit function.

The results of this research can assist in opening up the lines of communication and collaboration between the AC and the Chief Audit Executive (CAE) by serving as a starting point in a conversation to understand what it is that AC's require from internal audit reports.

In order to address the research objective presented above, a literature review and an empirical research study were performed. The literature review is presented in the next section and is divided into the following sub-sections:

- Defining the value that internal audit can add.
- Internal audit and the audit committee:
  - the internal audit function's reporting lines; and
  - the relationship between internal audit and the audit committee.
- Characteristics of an effective internal audit report:
  - the content of audit work communicated in the report; and
  - the quality of writing in internal audit reports.

3 LITERATURE REVIEW

3.1 Defining the value that internal audit can add

The glossary to the Standards (IIA 2012:22) defines the phrase *add value* as: "… when [the internal audit function] provides objective and relevant assurance and contributes to the effectiveness and efficiency of governance, risk management and control processes". Governance, risk management and control are fundamental to the definition of the internal audit function (IIA 2012:21). It is therefore axiomatic that for the internal audit report to increase the perceived relevance of the internal audit function, the internal audit report should itself be relevant and objective, and focus on the governance, risk management and control processes of the organisation.

According to Lenz and Sarens (2012:542), there is no *straightforward* answer to the question of what added value is. This could also indicate that the internal audit function does not have a clear understanding of what values stakeholders expect them to uphold and contribute to the organisation. The results of the PwC study (2011:3) reveal that an internal audit function adds significant value when it (internal audit function) is able to help management and AC understand the dynamic landscape of risks as well as to encourage a proactive behaviour to risks facing the organisation. Hence, it would seem advisable that internal audit should engage with its stakeholders to find out how they derive value from the internal audit reports, and internal audit should then ensure that addressing these issues becomes a significant component of their delivery.

Several studies have concluded that internal audit functions in general need to hold conversations with their stakeholders to explain how internal audit does (or should) in fact add value to the organisations (Mihret & Woldeyohannis 2008:14; PWC 2013:2; Ramamoorti 2003:15; Russell 2008:31). The same conversation should contribute to the internal audit function's understanding of what their (stakeholders) expectations of internal audit are. When there is a meeting of minds on expectations and their fulfilment, greater success in delivery is assured.

Whilst the Standards are silent on a definition of *value* as a deliverable, (and internal audit literature does not help much here either), the ultimate aim of the internal audit function is to improve their organisation's risk management, governance and control processes. These assessments and their remedies are communicated to the AC in the written internal audit report which then assists the AC to provide effective oversight of the internal audit function to the board.

The next section of the literature review examines the reporting structure supporting the internal audit function, and thereafter the roles of and relationships between the AC and the internal audit function are examined. The objective of the next section is to understand how internal audit can best assist the AC in fulfilling its responsibilities to the board.

3.2 Internal Audit and the Audit Committee

The internal audit function's reporting lines

The Standards require internal audit to report to a level within the organisation that allows it to fulfil its responsibilities (IIA 2012:7). In other words, the internal audit function should report to a level within the organisation that has the necessary influence to ensure the internal audit function can perform its tasks unhindered, and that its recommendations receive appropriate consideration.

Internal audit has dual reporting lines, reporting functionally to the AC and administratively to the Chief Executive Officer (CEO). King III (IOD SA 2009:97) supports this dual reporting relationship and recommends that internal audit also reports to the AC so that internal audit receives the respect and cooperation of the board and management.

The Basel Committee on Banking Supervision (under the auspices of the Bank for International Settlements) was established to address the shortcomings in the banking industry and has issued a guidance document on the role and importance of the internal audit function in banks. Principle 12 of the Basel Committee on Banking Supervision supports King III's view on the reporting structure and requires the internal audit function in a bank to be accountable to the board, or its AC, on all matters related to the performance of its mandate as described in the internal audit charter (BIS 2012:12).

King (2014:1) explains that internal audit is "the glue in modern governance and the right arm of the non-executive board". Hence, by positioning internal audit in an organisation so that it has a direct reporting line to the AC, increases the relevance and stature of the internal audit function.

The relationship between internal audit and the audit committee

The audit firm PFK (not dated:3) identifies the role of the AC as that of a "watchdog", and views it as a subcommittee of the board. The AC plays an oversight role over the integrity of financial controls, risk management and the transparent reporting to shareholders and stakeholders. King III (IOD 2009: 64) concurs with this allocation of responsibility, and in addition states that the AC needs to satisfy itself that the financial reporting risks, internal financial controls, fraud risk and information technology risks are appropriately managed in an organisation.

According to Schneider (2010:19) one of the main roles of the AC is to provide oversight of the internal audit function on behalf of the board. The board are responsible for risk management (RM) and control functions. And this responsibility is then delegated to the AC which is viewed as the central point for reporting on results of the audit (Paterakis & Cefaratti 2014:4; Sarens, De Beelde & Everaert 2009:2).

According to the Standards, the definition of IA includes the requirement "…to evaluate and improve the effectiveness of risk management, governance and control in organisations". It therefore appears that internal audit and the AC have interrelated objectives. The AC and internal audit need to develop a well-maintained channel of open communication so that internal audit can support the AC in its efforts to perform an effective oversight role (Paterakis & Cefaratti 2014:3; Rezaee & Lander 1993:37).

The document *The Audit Committee: Internal Audit Oversight* (IIA not dated:4) contains the assertion that ACs are required to have an in-depth understanding of business and associated risks, and of the environment in which that business operates. However, because internal audit is far closer to the operation of the business, it is more knowledgeable of the organisation's control environment, and is better able to understand the operating culture; the system of internal controls and the issues associated with business processes, as well as associated areas for improvement. It is precisely this knowledge that needs to come through when reporting to the AC on results of the audit.

Davies (2009:44) explains that ACs' responsibilities are increasing, driven by the increasing frequency of fraudulent scandals, new threats and risks. Internal audit functions need to be able to provide significant and relevant information so that ACs are able to meet their responsibilities. Achieving this leads to increased reliance being placed by ACs on the internal audit report, which in turn increases the relevance of the internal audit function.

According to Jacka (2014:71), Marks (2014:2), and Mihret and Woldeyohannis (2008:580), internal audit should communicate to its stakeholders what it is that their stakeholders need to know, and not what internal audit wants to say. The Institute of Internal Auditors Research Foundation (IIARF) (2013:7) asserts that CAEs should frequently ask AC members about their level of satisfaction with audit reporting. It is the responsibility of the heads of internal audit functions to communicate with their AC members and to tailor their reports to address the issues that the AC members need addressed.

Therefore for internal audit to remain relevant, it is important that internal audit understands the requirements of its customers (in this research restricted to the AC), and to provide them with the information that they need. By internal audit demonstrating their awareness of the different needs and preferences of their various stakeholders; this adds credibility to the reporting process and thus enhances the internal audit function's standing and authority in the organisation.

The next section of the literature review examines the characteristics of an effective internal audit report to an AC.

3.3 Characteristics of an effective internal audit report

The content of audit work communicated in the report

The International Professional Practices Framework (IPPF) of the Institute of Internal Auditors (IIA) includes 8 Standards under the heading *Communicating Results* (IIA 2012:18). Practice Advisory 2410-1 recommends that an internal audit report should include a fair assessment of both positive and negative aspects of the business and its environment, from the perspective of the engagement's scope and objectives. Furthermore, it should contain considered opinions based on the audit evidence, and conclude with recommendations to address root cause of issues identified.

A KPMG (2014:6) survey revealed that the audit reporting responsibility protocol has changed to be more transparent in the reporting of its external auditing and accounting issues. This involves including descriptions of key risks, an overview of the scope of the audit area, and an explanation of the method used by the auditor to address key risks.

Russell (2008:31) supports this view in internal audit, explaining that reporting to the AC is most effective when there is a clear explanation of the identified risks and of the probable impact of the audit findings.

The Chartered Institute of Internal auditors (CIIA) (2013:11) published a guide for financial services providers in the United Kingdom (UK) on how to enhance the effectiveness of the internal audit function. It should be noted that this guide is also useful to internal audit functions that are not in the financial services industry, as it provides a benchmark against which to measure their current functionality. The internal audit reports submitted to the board's audit and risk committees should, according to the CIIA, include the following areas:

- Provide a focused view on significant control weakness and breakdowns together with a root cause analysis.
- Highlight any thematic issues identified across the organisation.
- Provide an independent view of management's reporting on the risk management of the organisation, including a view on management's remediation plans (the view might include advising restricting further business improvements until plans have been successfully implemented), and highlighting areas where there are significant delays.
- Prepare, at least annually, an assessment of the overall effectiveness of the governance and risk and control framework of the organisation, together with an analysis of themes and trends emerging from recently completed IA work.

As these are seen by the industry as key components of an effective internal audit report, if the above issues are comprehensively addressed in the audit reports, this could increase the value of the internal audit report, which enables the AC to place greater reliance on their internal audit function's future reports. This ultimately creates a spiral of increasing relevance of the internal audit function.

Another important aspect of reporting, particularly to stakeholders, is its timing. Important and urgent information must be communicated as soon as possible. Prior to preparing the internal audit report, the auditor must also identify the intended audience, and tailor the report so that the issues it addresses are relevant to the recipients, and fall within the recipients' areas of responsibility and authority to take action (Rickard 1993:23; Schneider 2009:25).

The Standards require internal audit reports, to provide an overall opinion on the area under audit and to communicate clearly the evaluation criteria used in arriving at the opinion. The evaluation criteria are useful as it provides the AC with an understanding of how the overall opinion was derived.

Internal audit's (reporting) responsibilities can also include the education of the AC, achieved by including timeous information and reports on regulatory updates, changes in key suppliers, and assessments of the probable impact of changes in legislation (IIA nd:2; Schneider 2009:27). This type of pre-emptively provided information provides the AC with greater insight into the present and future state of the business, as the internal audit reports go beyond the (historic) issues identified during an audit. The inclusion of this type of information lends validity to the statement (made in the introduction to this research paper) that the internal audit function is the AC's eyes and ears in the business. Providing such information assists the AC in fulfilling its responsibilities when reporting to the board; and this will in turn increase the relevance of the internal audit function within the organisation.

Whilst it is essential that the content included in the audit report assists the AC in effectively discharging its duties, it is also important that the writing style in the reports is effective. The next section addresses the issue of appropriate styles of writing for reports.

The quality of writing in internal audit reports

Standard 2420 (IIA 2012:19) directs that the quality of communications must be "accurate, objective, timely, clear, concise, constructive and complete". Coetzee, Du Bruyn, Fourie and Plant (2010:261) state that there is nothing which loses appeal faster than a document with many grammatical and spelling errors. A document with many formatting and spelling errors draws attention away from the substance of the report (James 2014:1), thus diminishing the value of the report, and in turn, that of the internal audit function.

Standard 2420 (IIA 2012:19) directs that the quality of communications must be "accurate, objective, timely, clear, concise, constructive and complete". Coetzee *et al* (2010:261), James (2014:1), and Marks (2014:2) offer the following suggestions for achieving good business writing:

- Keep it simple - keep sentences short and [paragraphs] concise and free of technical jargon.
- The focus of the report should be on improvement rather than fault-finding and condemnation, and the tone should be without malice.
- Only pertinent information should be provided.
- Perform spell checks on written correspondence.
- Avoid use of unprofessional and slang words.
- The report should be written in the active voice - passive voice inspires little confidence.
- Proofread the document for accuracy of presentation of the intended message; check for and correct ambiguous sentences.
- Keep the tone of the writing professional, especially when raising exceptions.

In addition to the above, results of a roundtable discussion chaired by the IIARF revealed that internal audit reports should be "visually impactful" and make use of dashboards (a visual display of the most important information needed to achieve one or more objectives; and which can be monitored at a glance), heat maps (visual summary of information represented by colours) or summary graphics (IIARF 2013:7).

The next section explains the methodology that was adopted to collect evidence to support the research objective.

4 RESEARCH METHODOLOGY

In addressing the research objective presented in section 2 above, a structured research questionnaire was developed to collect the perceptions of the quality of content and writing of internal audit reports, held by AC chairpersons in the banking industry.

4.1 The research questionnaire

The questionnaire was developed from the knowledge and insight obtained from the literature review. The questionnaire was divided into 4 subsections: the first obtained demographic information; thereafter the sections explored the AC chairpersons' views on the quality of internal audit reports they receive, in terms of accurately conveying the content of audit work performed, and the writing style of the report.

A senior manager in quality assurance from one of the top 4 banks in South Africa reviewed the questionnaire, prior to sending it (questionnaire) out to the AC chairpersons. This was done to assess the completeness of the questionnaire.

The questionnaire made use of a combination of question styles, beginning with multiple choice questions and questions using a five-point response scale offering respondents the choice of *always/mostly/ seldom/never* and *not sure*. The AC chairpersons were required to select the response that he or she associated with the statement offered regarding various aspects of the internal audit reports they routinely received.

In addition to the question styles mentioned above, the questionnaire also had a section of open-ended questions, intended to give the AC chairpersons the opportunity to give their opinions on ways to improve the internal audit report, and thereby to increase the value of the internal audit function to their organisations.

4.2 Selection of respondents

The research population consisted of the AC chairpersons of 9 locally controlled banks and 2 foreign controlled banks (11 in total), all registered with the South African Reserve Bank (Reserve bank not dated:1). From this population positive responses were received from 4 of the locally controlled and the 2 foreign controlled banks.

4.3 Data collection

Each of the CAEs of the 11 banks was contacted via email to inform them of the intended research study, and to request their assistance in finding out whether their AC chairperson would be interested in completing the research questionnaire.

The CAEs were provided with 2 questionnaire delivery options: first, on receiving their agreement to assist, the questionnaire could be e-mailed directly to their AC chairperson; and second, the questionnaire could be sent to the CAE for forwarding to their AC chairperson.

Once approvals from the CAEs had been received, the questionnaire was sent via e-mail: From the population of 11 banks, a total of 6 approvals (from the CAE's) were received. Four went directly to the AC chairpersons, and two went first to the CAEs to be forwarded to their AC chairpersons. Four managed to meet the initial deadline. A follow up (reminder) email was sent to those who failed to meet the initial deadline for submissions, granting them an extra day.

4.4 Response rate

From the 11 CAEs that were approached, only 6 responded positively, confirming their AC chairpersons were willing to participate. This totals a response rate of 55% (6 out of 11).

4.5 Capturing and editing of data

The questionnaire was developed and emailed to respondents in MS Word format, and the six completed questionnaires were returned, via email, in the same format. The responses were then manually captured into an Excel spreadsheet for further analysis. The analysis of these results will be presented and discussed next, in section 5 of this research paper.

5 FINDINGS

The results of the questionnaire are presented and discussed in the same sequence as the questions were presented in the questionnaire:

5.1 Profiles of the audit committee chairpersons

5.2 Meetings and reporting relationship between audit committee chairpersons and CAEs

5.3 Content of information included in internal audit reports

5.4 Quality of writing style in internal audit reports

5.5 Recommendations to improve internal audit reports

5.1 Profiles of the audit committee chairpersons

Objective of the analysis

The objective of this part of the analysis was to determine the demographics of the respondents in terms of professional credentials, experience and access to internal audit reports.

Findings

Table 1 summarises the demographic information of the AC chairpersons.

Table 1: Profiles of the responding audit committee chairpersons

Criteria	AC chair 1	AC chair 2	AC chair 3	AC chair 4	AC chair 5	AC chair 6
Professional designation	CA. SA	CA. SA	CA. SA	CA. SA	CAIB(SA) -	CA. SA
Years of experience as AC chairperson in the banking industry	1.5	4	3	11	1	6
Unrestricted access to reports	Yes	Yes	Yes	Yes	Yes	No

Discussion of findings

The most frequently acknowledged qualification amongst respondents was the Chartered Accountant of South Africa (CA (SA)) designation, with only one respondent recording that she/he had a Chartered Associate of the Institute of Bankers qualification (CAIB) designation. The respondents' average number of years of experience as AC chairperson in the banking industry was 4 years. One respondent however, reported having been in the position for 11 years.

Five of the 6 respondents reported having unrestricted access to internal audit reports. The single respondent that did not have access to the internal audit reports also indicated in a subsequent section of the questionnaire that their IAF did not have a direct reporting relationship with the AC. This AC chairperson also reported only meeting with the CAE three times a year.

5.2 Meetings and reporting relationship between AC chair and CAE

Objective of the analysis

The objective of this part of the analysis was to determine the status of the internal audit function making use of the number of times the CAEs meet with the AC, and the functional reporting lines, as the definitive metrics.

Findings

Table 2 records the frequency of meetings between ACs and the CAEs as well as the reporting structures under which each of the respondents' banks' IAFs operate.

Table 2: Frequency of meetings and reporting structure

Criteria	AC chair 1	AC chair 2	AC chair 3	AC chair 4	AC chair 5	AC chair 6
Frequency of AC meetings with CAE per annum	4	6	5	4	4	3
CAE reports functionally to the AC Chairperson.	Yes	Yes	Yes	Yes	Yes	No
CAE consults with AC Chairperson on reporting requirements	Yes	Yes	Yes	Yes	No	No

Discussion of findings

Three out of 6 respondents reported having quarterly AC. This is favourable since the minimum frequency recommended by King III (IOD SA 2009:56) is for AC to meet twice a year.

Two of the 6 respondents (33%) reported meeting more than 4 times a year. It might be significant that, as reported in the next sections, their responses to the content and writing style of the audit reports they receive is positive.

Five of the 6 respondents (83%) indicated that the CAE reports directly to them. As supported in the literature review, the stature of the IAF is enhanced when direct reporting lines are in place.

Four out of 6 respondents (67%) confirmed that the CAE does consult with them to identify their (the AC chairperson's) requirements from the IAR. It was also evident in the responses to subsequent questions (presented in Table 3, Table 4.1 and Table 4.2) that the greater the frequency of consultations between the CAE and the AC chairperson, the greater the completeness of content and writing style was apparent in the responses; This increases the reliance the AC chairperson was able to place on the internal audit report, which in turn increased the perceived relevance of the IAF.

5.3 Content of information included in the internal audit report

Objective of the analysis

The objective of this section was to identify the current content that AC chairpersons receive from their internal audit reports and to compare this to the ideal content revealed in the literature review.

Findings

Table 3 provides a summary of the ACs chairpersons' responses with respect to how often such ideal content is included in the internal audit reports they receive.

Table 3: Content of internal audit reports

	Percentage is out of the sample (6)					
	Always	Mostly	Seldom	Never	Not sure	Total
a) Only significant control gaps and break downs.	100%					100%
b) Root cause analysis	33%	50%				83%*
c) A scope statement	67%	17%	17%			100%
d) Analysis of themes and trends	50%	33%	17%			100%
e) Possible risks that could occur in the future	17%	17%	67%			100%
f) Details of any fraud discoveries	83%	17%				100%
g) Alerts to red flag indicators	33%	33%	17%	17%		100%
h) Reasons for significant delays by management in responding to reports requiring implementation of corrective actions.	67%	33%				100%
i) Overall audit opinions on the area under audit are accompanied by clear evaluation of the criteria used in expressing such opinion.	33%	67%				100%
i) Reports are balanced and include the positive control practices as well as the control weaknesses observed.	83%	17%				100%

*One respondent only recently commenced with this inclusion.

Discussion of findings

The majority of responses fell between the *always* and *mostly* points on the response scale. However on the issue of *possible risks that could occur in the future* 67% (four out of 6 respondents) claimed that this was *seldom* included in the report. Another concerning response is with regard to *alerts to red flag indicators;* one respondent selected the seldom option, whilst one other respondent claimed to never include such content. As this aspect of the report has been identified in the literature review as "significant value", local internal audit functions should look to including this in their internal audit reports as it allows AC chairpersons to alert the board on specific future risk possibilities and also to provide an overall picture of the risk universe confronting the organisation.

AC chairpersons have a reporting responsibility to the board which is more efficiently fulfilled when the internal audit report on matters that warrant the attention of the board contains just that. It was therefore reassuring to see that **all** respondents selected *always* in response to the question whether the audit reports included "only significant control gaps and breakdowns". This ability on the part of the internal audit function builds credibility for the internal audit function, allowing the AC to rely on internal audit to highlight matters of significance.

In searching for correlations between the data presented in Table 2 and that of Table 3 it became apparent that the guidance provided by the Chartered Institute of Internal auditors (CIIA) (2013:15) and the IIA's Practice Advisory 2410-1 are not consistently applied by the banks participating in this research study.

5.4 Quality of writing style in internal audit reports

Objective of the analysis

The objective of this part of the analysis was to determine and assess the characteristics of the internal audit reporting characteristics and the writing style of the internal audit report that best assist the AC to provide the board with information appropriate to ensuring effective oversight of the business.

Findings

Table 4.1 summarises the AC chairpersons' responses to the suggested characteristics included in the internal audit report that would then enable them (AC chairpersons) to report most effectively to the board.

Table 4.1: Internal audit reporting characteristics

	Percentage is out of the sample (6)					
	Always	Mostly	Seldom	Never	Not sure	Total
a) The communication is concise and avoids unnecessary elaboration, superfluous detail and redundancy.	33%	67%				100%
b) Technical and buzz words are avoided.	17%	67%	17%			100%
c) The impacts of findings are appropriately worded to warrant attention.	67%	33%				100%
d) The reporting of significant items is timeous.	33%	67%				100%
e) The report provides greater insight into the interconnectedness of business processes	17%	33%	50%			100%
f) The recommendations address the root causes of issues.	33%	33%	17%			83%*

*One respondent only recently commenced with this inclusion.

Discussion of findings

For the majority of the audit report characteristics, the responses selected were *always* and *mostly,* the top end of the scale, with remaining respondents selecting the *seldom* option. This indicates that no single standard or consistent application of these reporting characteristics is being implemented in the respondents' banks.

The responses to characteristics e) and f) above showed a greater range than the preceding 4 characteristics did, suggesting that these are areas where IA can expend more effort in seeking improvement. In so doing the AC is better equipped to understand the risk universe of the organisation which will enhance the internal audit function's perceived usefulness and credibility.

The data shows to users of the internal audit report that internal audit does have a useful understanding of the entire organisation, but with "room for improvement". Overall they are therefore in a position to provide connected insights arising from the performance of their audit engagements (PwC 2011:18).

Findings

Table 4.2 provides a summary of the general quality of writing style included in internal audit reports.

Table 4.2: General writing style apparent in internal audit reports

	Percentage is out of the sample (6)					
	Always	**Mostly**	**Seldom**	**Never**	**Not sure**	**Total**
a) Tone of reports focuses on improvement, rather than condemnation.	67%	17%	17%			100%
b) The report is written in active voice.	33%	50%			17%	100%
c) The report is free of errors in spelling and grammar.	50%	50%				100%
d) The reports are supported by visual aids such as dashboards or heat maps or summary graphics.	33%	50%		17%		100%

Discussion of findings

Overall the responses reveal that the writing style used in internal audit reports is diverse and spans the full range of options offered the respondents. However, the majority of responses placed the internal audit reports style elements in the *always* and *mostly* categories.

Regarding spelling and grammar, only half the respondents gave their internal audit reports an *always* assessment (report characteristic c) in Table 4.2. This is problematic since, as noted by Coetzee *et al* (2010:261) and James (2014:1) a report that has errors in spelling and grammar loses its appeal, which tends to decrease the perceived value of the report, and introduces the risk that the substance of the matters it addresses will be missed.

One respondent also indicated that visual aids are *never* incorporated into the report. This is despite the fact that the IIARF (2013:7) supports the use of heat maps in reports, as they make the report visually impactful.

5.5 Recommendations to improve internal audit reports

Objective of the analysis

The objective of this part of the analysis was to offer respondents a platform for their ideas on how the internal audit report can be improved so as to increase the value of the internal audit function. Respondents were asked: '*Please provide any feedback on how you think the current internal audit reports can be improved to add value to the internal audit function?'*

Findings and discussion

Four of the 6 respondents (67%) were very positive and forward-looking, which indicates that the AC chairpersons do rely on the internal audit reports to provide them with insightful opinions that in turn allow them to report effectively to the board on internal audit matters. The remaining 2 respondents indicated that they were "happy" with the style and presentation of their current reports and did not require additional input or improvements. However when the other two respondents assessment of content and writing style are compared with the other four, and factoring in the other parameters measured in this research, these two respondents appear to have internal audit functions that are below average in terms of their current reporting capabilities.

A common response from all 6 respondents was that the AC requires less "unnecessary information", and that low residual risk reporting should be kept to a minimum. Achieving this would be a significant improvement in the internal audit reports they receive.

One respondent observed that the internal audit report was "constantly evolving". This is an interesting statement, probably indicating that the AC chairpersons are aware that the internal audit function operates in an environment of constant change and necessary improvement. The internal audit function therefore also needs to keep abreast of reporting trends, while simultaneously keeping up to date with the needs and expectations of AC chairpersons in order to remain relevant and to contribute value to their organisations.

6 FURTHER RESEARCH

An area for further research is to conduct a qualitative study to determine how the content and writing style of internal audit reports can be improved so as to enhance the credibility of the internal audit function.

7 CONCLUSION

The internal audit report is considered to be the final outcome or deliverable of the internal audit engagement. The objective of this research paper was to identify the current perceptions of the banking industry's AC chairpersons of the substance and quality of the content and writing style of the internal audit reports they receive. A literature review was conducted to identify the most pertinent factors that the internal audit function should consider when preparing their internal audit reports.

From a content perspective the following issues need to be addressed in order to increase the relevance of the report, and by extension, the internal audit function itself. The internal audit function should engage with its stakeholders to find out what they need from internal audit reports: the literature review maintains that reports should be concise and precise, highlighting significant control gaps and breakdowns; provide root cause analyses; analyse emerging trends, and provide insight on emerging and potential risks.

From a writing perspective, the following factors should be considered when preparing internal audit reports. The report should be free of spelling and grammatical errors; it should be a concise communication and avoid the use of technical jargon and buzz words, and should display the internal audit function's insightful overview of the connections within and between the business' processes.

The questionnaire responses revealed unanimity only insofar as all the internal audit reports apparently reported on significant control gaps and breakdowns. Only one respondent appeared to be consistent in their assessment of content and writing style of the reports they receive, whilst the others, by selecting 'mostly' and 'seldom' indicated that there is still (sometimes significant) room for improvement. Therefore there is still plenty of room for improvement in the quality of internal audit reports that are currently being submitted to AC chairpersons.

However, the fact that six out of a population of 11 AC chairpersons chose to respond to the questionnaire suggests that a majority of AC chairpersons do recognise that the internal audit report has value, but that it also has the potential for significant improvement. This should encourage CAEs to work together with the AC chairpersons in order to deliver a report which feeds directly and efficiently into the ACs communication to the board.

The internal audit report serves as the communication tool which provides the AC with the raw material needed for its report to the board. By preparing an effective, value-rich audit report which takes into account the specific needs of the AC, while simultaneously addressing the style and content factors identified in the literature review, should enable the internal audit function to enhance its relevance within the organisation.

REFERENCES

BIS: See Bank for International Settlements.

Bank for International Settlements. 2012. *The internal audit function in banks*. [Online]. http://www.bis.org/publ/bcbs223.pdf (Accessed 16 July 2012).

Chartered Institute of Internal Auditors (CIIA). 2013. *Effective Internal audit in the Financial Services sector*. [Online]. http://na.theiia.org/standardsguidance/Public%20Documents/Effective%20Internal%20Audit%20Financial%20GLOBAL.pdf. (Accessed 08 August 2014).

CIIA: See Chartered Institute of Internal Auditors.

Coetzee, P., Du Bruyn, R., Fourie, H. & Plant, K. 2010. *Advanced Internal audit topics*. Durban: LexisNexis.

Davies, M. 2009. Effective working relationships between audit committees and internal audit – the cornerstone of corporate governance in local authorities, a Welsh perspective. *Journal of Management & Governance*,13(1/2):41-73.

IIA: See The Institute of Internal Auditors.

IIARF: See The Institute of Internal Auditors Research Foundation.

Institute of Directors. 2009. The King III report and code on governance in *South Africa* (3). South Africa: LexisNexis.

Jacka, M. 2014. Trying to solve the wrong problem. *Internal Auditor*, LXXI:II:71.

James. S, 2014. *Simple steps for better reports*. [Online]. http://audit&risk.org.uk/tools/simple-steps-for-better-reports [Accessed: 2014-09-03].

Kapoor, G. & Brozetti, M. 2012. The transformation of internal auditing. *The CPA Journal*, 82(8):32-35.

King III: See *Institute of Directors.*

King, M. 2014. *Survival guide.* [Online]. http://auditandrisk.org.uk/features/survival-guide (Accessed: 04 September 2014).

KPMG. 2014. *Audit committees' and auditors' reports. A short survey of the new reporting*. [Online]. http://www.kpmg.com/UK/en/IssuesAndInsights/ArticlesPublications/Documents/PDF?Issues%20and%20Insights/audit-comm-audit-reports.pdf (Accessed: 03 September 2014).

Lenz, R. & Sarens, G. 2012. Reflections on the Internal auditing profession: What might have gone wrong? *Managerial Auditing Journal*, 27(6):532-549.

Marks, N. 2014. Effective Internal audit reports. *IIA online communicator.* [On-line]. http://iaonline.theiia.org/ effective-internal-auditreports. (Accessed: 04 September 2014).

Mihret, D. & Woldeyohannis, G. 2008. Value added role of internal audit: an Ethiopian case study. *Managerial Auditing Journal*, 23(6):567-595.

Paterakis, N. & Cefaratti, M. 2014. Strengthening Audit Committee Communication: Internal and External audit communication guidance. *Internal Auditing Communication Guidance*, 29(2):3-7.

PFK. not dated. The Audit Committee. Companies Act 71 of 2008. [On-line]. http://www.pfk.co.za/media/ 150546/audit_committee_e_.pdf (Accessed: 30 July 2014).

Plant, K. & Steyn, B. 2010. The status and demand for internal auditing in South African companies. IKUTU research report. [On-line]. https://www.cass.city.ac.uk/_data/assets/pdf_file/0018/37332/Kato-Plant.pdf (Accessed: 10 July 2014).

PricewaterhouseCoopers (PwC). 2011. *State of the Internal Audit Profession Study. Maximising the value of Internal Audit: who dares wins.* [Online]. http://www.pwc.com.au/assurance/assets/MaximisingValue-who-dares-wins Sep11.pdf (Accessed: 22 March 2014).

PricewaterhouseCoopers (PwC). 2013. *State of the Internal Audit Profession Study. Reaching greater heights: Are you prepared for the journey?* [On-line]. http://www.imfo.co.za/downloads/june2013/PwC%20IMFO% 202013%20Risk20Management%20Rudolf%20JoosteSOTP.pdf (Accessed: 15 October 2015).

PricewaterhouseCoopers (PwC). 2014. State of the Internal Audit Profession Study. *Higher performance by design: A blue print for change* [On-line]. http://www.pwc.com/en_M1/m1/publications/documents/pwc-state-of-the-internal-audit-profession-2014.pdf (Accessed 22 July 2014).

PwC: See PricewaterhouseCoopers.

Ramamoorti, S. 2003. *Internal Auditing: History, Evolution, and Prospects*, IIA Research Foundation, Altamonte Springs, FL. [On-line]. http://na.theiia.org/iiarf/Public%20Documents/Chapter%201%20Internal%20Auditing%20History%20Evolution%20and%20Prospects.pdf (Accessed: 22 March 2014).

Reserve Bank: See South African Reserve Bank.

Rezaee, Z. & Lander, G.H. 1993. The internal auditor's relationship with the audit committee. *Managerial Auditing Journal*, 8(3):35-40.

Rickard, P. 1993. Audit reports in the 1990s. *Australian Accountant*, 63(1):19-23.

Rittenberg, L. 2002. Lessons for internal auditors. *The Internal Auditor*, 59(2):32.

Russell, G. 2008. Internal Audit revisiting the value agenda. *Accountancy Ireland*, 40(4):3133.

Sarens, G., De Beelde, I. & Everaert, P. 2009. Internal audit: A comfort provider to the audit committee. *The British Accounting Review*, 41:91-106.

Schneider, A. 2009. Informing The Audit Committee: Information and Reports Provided By Internal Audit, *Internal Auditing*, 24(2):24-32.

Schneider, A. 2010. Assessment of Internal Auditing by Audit committees. *Academy of Accounting and Financial Studies Journal*, 14(2):19-26.

South African Reserve Bank. Not dated. *South African Registered Banks and Representative Offices.* [Online]. https://www.resbank.co.za/RegulationAndSupervision/BankSupervision/Pages/SouthAfricanRegisteredBanksAndRepresentativeOffices.aspx (Accessed 26 October 2014).

The Institute of Internal Auditors (IIA). 2014. *Enhancing value through collaboration: A call to action. Audit Executive Center*. [Online]. http://global.theiia.org/memberresources/Global%20Documents/2014%20Global%20Pulse%20of%20the%20Profession%20-%20Enhancing%20Value%20Through%20Collaboration%20-20A%20Call%20to%20Action.pdf (Accessed:17 September 2014).

The Institute of Internal Auditors (IIA). 2012, The International Standards for The Professional Practice of Internal Auditing (Standards). [Online]. http://global.theiia.org/standards-guidance/Public%20Documents/IPPF%202013 %20English.pdf (Accessed 15 May 2013).

The Institute of Internal auditors, not dated. *The Audit Committee: Internal Audit Oversight.* [Online]. http://na.theiia.org/about-ia/PublicDocuments/08775_QUALITY-AC_BROCHURE_1_FINAL.pdf (Accessed 2014).

The Institute of Internal Auditors Research foundation, 2009. *The Financial Crisis and Its impact on the Internal audit profession*, Global Audit Information Network (GAIN). [Online]. www.theiia.org/download.cfm?file=82635 (Accessed: 04 September 2014).

The Institute of Internal Auditors Research foundation (IIARF), 2013. The Audit Committee and the CAE. Sustaining a Strategic partnership [Online]. http://www.theiia.org/bookstore/downloads/freetomembers/ 1171788_ AC%20and%20the%20CAE.pdf (Accessed: 04 September 2014).

Whitfield, B., 2014. African Bank’s demise entirely predictable. *The Sunday Times*, Business section, 10 August: 7.

The Southern African Journal of Accountability and Auditing Research

Evolving Research

Perspectives of chief audit executives on the implementation of combined assurance

H K Schreurs
Department of Auditing
University of Pretoria

M Marais
Department of Auditing
University of Pretoria

ABSTRACT

This article explores the status of current combined assurance practices as experienced by the chief audit executives (CAEs) of listed companies in the financial services industry in South Africa. The study aims to determine the status of combined assurance, to identify critical success factors for the implementation of combined assurance, to determine the role of internal audit in the implementation of combined assurance, and to identify limiting factors that may hamper the success of the combined assurance process as described in the literature and experienced by the chief audit executives (CAEs) of the companies surveyed.

The results of the study indicate that combined assurance implementation is seen as a journey, and that organisations are still at various levels of maturity in the implementation process. Organisations struggling with full implementation identified the following as limiting factors: a lack of buy-in from executive management; immature second line of defence functions; different regulatory environments, and the lack of a combined assurance champion. Key foundational areas identified as requisite for successful implementation related to appointing a combined assurance champion and an executive sponsor, mature first and second line of defence functions, formal statements of roles and responsibilities of assurance providers, and buy-in and active participation from the audit committee chairperson.

Key words

Internal auditing; combined assurance; chief audit executives; three lines of defence; financial services industry

1 INTRODUCTION

Historically, assurance providers have carried out their assurance activities in silos. This approach resulted in assurance activities being shared by management, risk management, regulatory risk management, internal audit and external audit, but without the coordinating activities and resources required to ensure the provision of effective and efficient combined assurance (IIA 2012:4). The risks affecting today's organisations are so diverse that this approach is no longer adequate. Indeed, a silo approach has been found to result in inefficiencies in risk management, as well as a lack of consistency and transparency in assurance services (Sarens, Decaux & Lenz 2012:xi).

In order to break away from the silo approach, the third King Report on Governance for South Africa (King III) suggested, in 2009, the development of a complementary relationship between assurance providers under the coordination of the audit committee, terming this relationship 'combined assurance' (Institute of Directors 2009). King III defines combined assurance as the integration and alignment of assurance processes in a company in order to maximise the risk and governance oversight and control efficiencies, and to optimise the overall assurance given to the audit and risk committees, taking into account the company's risk appetite (Institute of Directors 2009:50).

Turlea, Mocanu and Radu (2010:397) describe a complementary relationship between the audit committee, internal audit, and external audit as a relationship where each of these areas, by carrying out their respective roles and responsibilities in an organisation, complete and sustain each other as part of effective corporate governance.

The objective of combined assurance is to satisfy the audit committee that the combined efforts of all assurance providers are sufficient to provide assurance that all significant risk areas have been addressed adequately and that controls exist to mitigate these risks (PWC 2011:4; Deloitte 2012:11).

2 RESEARCH OBJECTIVES AND METHODOLOGY

2.1 Objectives and significance of this article

Literature on combined assurance is limited owing to the fact that it is a fairly new concept (introduced to

South Africa's corporate environment in 2009) and a practice that has thus far been primarily carried out on an informal or trial basis in South Africa. In addition to analysing and summarising the available literature on combined assurance, this article aims to add to the existing literature on current practices by providing insights gained from an empirical study performed to explore the status of current combined assurance practices in the financial services industry in South Africa. The objectives of this empirical study were to establish the status of combined assurance; to identify critical success factors for the implementation of combined assurance; to determine the role of internal audit in the implementation of combined assurance; and to identify limiting factors that may hamper the success of the combined assurance process as described in the literature and experienced by the chief audit executives (CAEs) of the companies surveyed.

This article may assist companies in South Africa with their implementation of combined assurance and may help to improve the effectiveness of existing combined assurance efforts. The article can also be used to obtain a better understanding of the critical success factors that have to be present if the effective implementation of combined assurance is to take place.

2.2 Research methodology and limitations

The research supporting this article consisted of a combination of a literature review and an empirical study. The literature review involved a study of guidelines, informative articles, and research publications in scholarly journals on the topic of combined assurance and other related issues concerning the nature of combined assurance, as well as critical success factors in the implementation of combined assurance. The literature review served both to inform the empirical study and to supplement its findings.

The study follows a mixed methods approach, which is described by Creswell (2009:77) as a method that "brings together approaches that are included in both quantitative and qualitative research formats." According to Creswell (2009:14), the concept of mixing different methods was introduced by Campbell and Fick in 1959, who found it to be so useful that they encouraged other researchers to also examine multiple approaches to data collection. The benefit of using a mixed methods approach is that the results of the quantitative survey can help to identify issues or questions to explore further during interviews with respondents, which then add qualitative insights to the research (Creswell 2009:14).

The quantitative side of the research involved a self-administered, cross-sectional survey that intended to collect data at a certain date and time (Creswell 2009:146). A questionnaire, specifically designed for the purpose of the study, served as the research instrument. After its initial design the questionnaire was presented to academics for their input and then tested by the researchers. Permission was obtained for the distribution of the questionnaire from the individual respondents before the questionnaires were electronically mailed to them.

The questionnaire was purposefully distributed to the CAE in each company, as they have been identified in the literature as a party that plays an important role in combined assurance. It was assumed that their role in combined assurance and their holistic view of the organisation's operations would enable them to provide meaningful perspectives of the combined assurance practices in their organisations.

Once the completed questionnaires had been analysed, structured follow-up interviews were held with each of the respondents to obtain a more in-depth view of their experiences and perceptions regarding the implementation of combined assurance in their organisations. These interviews, fulfilling the research methodology's requirements for a quantitative component, added valuable insight into the critical factors for implementing combined assurance and the challenges experienced in doing so.

2.3 Sample selection and response rate

The sample population was stratified to include only companies in the financial services industry in South Africa with either a primary listing, a secondary listing, or a dual listing on the Johannesburg Stock Exchange Limited (JSE). From this population the participants were purposefully selected to include the biggest companies in the financial services industry in South Africa, based on market capitalisation. The companies thus selected included the eight largest banking, life insurance, and general financial services companies in South Africa, representing 70.72% of the market capitalisation of the financial services industry as of 12 September 2014 (Beeld 2014:15). The companies included in the sample represented 76.40% of the market capitalisation of listed companies in the banks sector of the JSE, 77.67% of the market capitalisation of listed companies in the life insurance sector of the JSE, and 37.47% of the market capitalisation of the general financial sector on the JSE.

The response rate achieved for this study was 100%, although usable responses in the form of completed questionnaires and follow-up interviews represented 87.5% of the population surveyed, as depicted in Table 1. One of the CAEs of the eight companies selected indicated that their company had not implemented combined assurance entirely and they would therefore not complete the questionnaire. A limited follow-up interview was subsequently held with this CAE.

2.4 Limitations of the empirical study

The study was limited to the financial services industry in South Africa. Within this industry the study focused on the banks, life insurance, and general finance sectors, as defined by the JSE. The findings may therefore not be representative of all life insurance and banking institutions in South Africa, and may also not be representative of the state of combined assurance in other industries in South Africa.

Another limitation is that the study only measured the views and perceptions on the state of combined assurance, as provided by the CAEs of the companies included in the study, and no other stakeholders or participants in the three lines of defence were included. The views of other participants in the combined assurance process, for example non-executive directors, audit committee members, and the audit committee chairman, as well as the other assurance providers may therefore differ from those expressed by the CAEs.

Table 1: JSE sector classification of companies selected for the survey and questionnaires completed

JSE Sector	Number of companies selected	% of companies selected	Number of surveys completed	% usable responses from companies selected
General Financial	1	12.50	1	12.50
Banks	4	50.00	4	50.00
Life Insurance	3	37.50	2	25.00
	8	**100.00**	**7**	**87.50**

3 LITERATURE REVIEW

During the study of the available literature on the topic of combined assurance three predominant themes for discussion were identified: introducing the concept of combined assurance and clarifying its purpose in organisations; determining roles and responsibilities for combined assurance efforts, and identifying critical success factors for the implementation of combined assurance.

3.1 Introducing the concept of combined assurance and clarifying its purpose in organisations

In 2009, King III introduced the concept of combined assurance to the South African governance landscape with the inclusion of principle 3.5. This principle states that the audit committee should ensure that a combined assurance model is applied so as to provide a coordinated approach for all assurance activities (Institute of Directors 2009:33). Also in 2009, the Institute of Internal Auditors Global (IIA) introduced the principle of combined assurance with the release of Practise Advisories 2050-1: *Coordination*, and 2050-2: *Assurance maps* (IIA 2009). These standards of practice primarily require the CAE to share information and coordinate activities with other internal and external providers of assurance, to ensure proper coverage and minimise the duplication of effort.

The coordination of activities between internal auditors and other assurance providers, such as external auditors, has been a point of discussion for quite some time (Brody, Golen & Reckers 1998:161; Tapestry Networks 2004:6; Sarens & De Beelde 2006:67; Porter 2009:178; Schneider 2009:41). This practice is addressed in the professional standards of both internal and external audit disciplines. Internal Auditing Standard 2050: *Coordination* states that the CAE should share information and coordinate activities with other internal and external assurance providers to ensure adequate coverage and to minimise duplication of effort (IIA 2009:133). International Standard on Auditing 315 – *Identifying and assessing the risk of material misstatement through understanding the entity and its environment* (IAASB 2013:305) – allows external audit to reduce the extent and to modify the nature and timing of audit procedures on the basis of the assurance activities conducted on the entity's financial reporting controls by internal audit. International Standard on Auditing 610 – *Using the work of internal auditors* (IAASB 2013:637) – allows external auditors to rely on the work performed by the internal audit function, depending on whether the function's level of competency is adequate and whether it applies a systematic and disciplined approach to assurance.

Factors that necessitate a greater emphasis on the integration of internal and external audit include the understanding that effective corporate governance can minimise the risk of corporate collapse. In addition, it can curb the increase in assurance costs, and the need for high-quality auditing (Munro & Stewart 2010:466; Mihret & Admassu 2011:67). Research conducted by Felix, Audrey, Gramling and Maletta (2001:514) concluded that the coordination of the activities of internal and external auditors increases the effectiveness of overall assurance and minimises duplication of effort. Mihret and Admassu (2011:68) add that coordination between internal and external audit should also result in lower audit risk. According to guidance on the 8th EU Company Law Directive, provided by the European Confederation of Institutes of Internal Audit (ECIIA) and the Federation of European Risk Management Associations (FERMA), internal and external auditors should meet regularly to discuss their scopes of work, methodologies, and audit coverage (ECIIA FERMA 2010:17).

However, combined assurance, as described in King III, requires the coordination of *all* assurance providers and, as such, is a fairly new concept. While external auditors provide the company's shareholders with reasonable assurance that the financial statements are free from material misstatements (IAASB 2013: 679), internal auditors are required to attest to the reliability of the internal control system, including the financial controls (IOD 2009:45), and the maturity of risk management in the organisation (Fraser & Henry 2007:396; IOD 2009:45; IIA 2012:2). The role of other assurance providers – such as management – involves identifying, assessing, evaluating, controlling, and managing risks (Sarens & De Beelde 2006:65; IIA 2013:3), while the risk management and regulatory risk management functions facilitate and monitor both the effective implementation of risk management practices and non-compliance with applicable rules and regulations (IIA 2013:4).

3.2 Determining roles and responsibilities for combined assurance efforts

From the literature study it is clear that a combined and coordinated approach is recommended for the effective implementation of combined assurance. In combined assurance all the role-players are considered equally important and include the stakeholders, assurance providers, and coordinators of the process.

3.2.1 Stakeholders

The board and the audit committee are the primary stakeholders in combined assurance (IOD 2009:33). It is therefore vital for them to be involved in the implementation of frameworks and processes for combined assurance (IIA 2013:2).

Roles that have been identified for the **board** in combined assurance are: to provide oversight and direction to management by setting the risk appetite and risk tolerance levels (IOD 2009:36; ECIIA FERMA 2010:7; Sarens *et al* 2012:12); to set organisational objectives and define strategies, and to implement them by establishing appropriate governance structures to manage risk (IIA 2013:3); to be aware of the significant risks in the organisation (ECIIA FERMA 2010:7); and to monitor the way in which management responds to these significant risks (ECIIA FERMA 2010:7; PWC 2013:7).

The **audit committee**'s roles include overseeing the work performed by, and the coordination between, internal and external audit, reviewing and receiving feedback on audit reports that identify weaknesses in the control environment, and reviewing management's responses (Porter 2009:176; Turlea *et al* 2010:396; Sarens *et al* 2012:13). Audit committees also have to provide reports on compliance with the organisation's statutory duties, assess the independence of external audit in providing a view on the financial statements and the application of accounting practices, ensure the integrity of integrated reporting, and assess whether internal financial controls have been effective (IOD 2009:32; ECIIA FERMA 2010:6; Roos 2012:31; PWC 2013:26).

Shareholders have also been identified as a stakeholder group because, as legal owners, they are protective of their investments in the organisation (Lyons 2011:7). Shareholders cannot control the board or the audit committee directly, but exert their influence as a collective by exercising their rights through the annual general meeting. Shareholder activism has in recent times become an effective tool for demanding changes. This is accomplished through exercising shareholder rights at the annual general meeting (Lyons 2011:7).

3.2.2 Assurance providers

Combined assurance formalises the roles and responsibilities of the various assurance providers in relation to each other in terms of three lines of defence. In January 2013 the IIA released their position paper on this matter, entitled *The three lines of defence in effective risk management and control*. This position paper states that specific roles and responsibilities should be assigned to the various assurance groups to ensure that there are no gaps in or duplication of the assurance activities (IIA 2013:1).

The literature review indicates that the Bank for International Settlements (BIS) was the first to introduce the concept of three lines of defence in the effective risk management practices for banks (BIS 2011:3). Accordingly, BIS identified business' line management as the first line of defence, an independent operational risk management function as the second line, and an independent review function as the third line. The IIA position paper (IIA 2013:3) recommends classifying the lines of defence according to the related functions; thus owning and managing risk (first line), overseeing risk (second line), and providing assurance on controls implemented to mitigate risk (third line).

The IIA position paper further claims that the basic objective of the three lines of defence in combined assurance is to ensure that collectively, all three lines of defence will identify and mitigate the organisation's critical risks before they penetrate the organisation. It is essential therefore that the boundaries of each assurance provider's role be clearly understood, as well as the way in which their position fits into the organisation's overall control structure (IIA 2013:7).

Management ultimately owns and manages risks within the organisation and is commonly seen as the first line of defence (Sarens *et al* 2012:18; IIA 2013:3). The inclusion of management in the first line of defence acknowledges management's ownership and recognises its importance in setting the "tone at the top" in relation to good corporate governance (Gramling, Maletta, Schneider & Church 2004:198). Management identifies, assesses, controls, and mitigates risk by developing policies and procedures and by implementing controls that ensure that risk is reduced to levels that are acceptable to the risk appetite of the organisation (ECIIA FERMA 2010:3; Lyons 2011:2; Daugherty & Anderson 2012:39; IIA 2013:3).

The second line of defence typically consists of functions such as enterprise risk management, regulatory risk management, fraud risk management, Sarbanes-Oxley (SOX) compliance officers, health and safety officers, and environmental review officers, as well as insurance, ethics and legal functions (PWC 2010:7; IIA 2013:2; Corporate Executive Board 2013:3). Assurance providers in the second line of defence monitor and facilitate the implementation of effective risk management practices, and assist in the adequate reporting of risks through the governance structures (ECIIA FERMA 2010:4). Their role is therefore to assist management in monitoring and managing risk. Second-line defenses also assist in the implementation of risk responses and monitor effective risk management practices across the organisation (IIA 2013:4). Additional responsibilities such as training, policy and framework setting, and control assessments may also be assigned to the second line of defence (Daugherty & Anderson 2012:39).

The third line of defence generally consists of the internal and external audit functions (PWC 2010:14; Sarens *et al* 2012:19; EY 2013:4). In some approaches external audit is not considered to be part of the third line of defence, as it is independent of the organisation; nevertheless it is still regarded as delivering a core assurance service in the organisation, aligning and coordinating its assurance efforts with the other internal assurance providers (Lyons 2011:6; ECIIA 2012:4; IIA 2013:6).

In most organisations internal audit would be the primary assurance provider in the third line of defence (PWC, 2010:14; Sarens *et al* 2012:19; EY 2013:4). Spira and Page (2003:649) support this view, maintaining that internal audit is in the best position to understand the entire organisation's internal control systems and control environment. Indeed, Practise Advisories 2050-1: *Coordination* and 2050-2: *Assurance maps* (IIA 2009) require the CAE to be part of the organisation's assurance provider framework, and the practice guide *Coordinating Risk Management and Assurance* issued by the Institute of Internal Auditors (IIA 2012) requires internal audit to report to the board on the effectiveness of the risk management function. King III's principle 7 also recommends that internal audit should provide the board with an annual written assessment of the internal control and risk management systems and, in addition, provide the audit committee with an assessment of internal financial controls (IOD 2009:45). Fraser and Henry (2007:396) note that this responsibility requires the internal audit function to have an in-depth understanding of enterprise risk management, while PriceWaterhouseCoopers (PWC) (2010:11) holds the view that internal audit will not be able to meet this responsibility without aligning with, and placing reliance on, testing that has been performed by other assurance providers.

3.2.3 Coordinators

The literature agrees that a combined assurance champion needs to be appointed to drive and implement combined assurance (PWC 2011:6; Lyons, 2011:5; Sarens *et al* 2012:29; Daugherty & Anderson 2012:41). The most popular nominations for this position are the audit committee and internal audit.

King III recommends that the audit committee should coordinate combined assurance in organisations. Thus, Principal 3.5 states:

> "The audit committee should ensure that a combined assurance model is applied to provide a coordinated approach to all assurance activities.
>
> 3.5.1. The audit committee should ensure that the combined assurance received is appropriate to address all the significant risks facing the company.
>
> 3.5.2. The relationship between the external assurance providers and the company should be monitored by the audit committee.*"* (Institute of Directors 2009)

Coordinating combined assurance implies that the audit committee will have a dual responsibility in combined assurance, namely, as a primary stakeholder and as the coordinator. Coordinating combined assurance adds the following to those responsibilities identified earlier for the audit committee in an organisation: reviewing the effectiveness of and cooperation between the three lines of defence (Lyons 2011:5); periodically reviewing the assurance structure to ensure that all the needs of the various stakeholders are met, and ensuring that all critical business risks are mitigated (KPMG 2012:6).

The ECIIA (ECIIA 2012:2) recommends that audit committee oversight should rely on an all-embracing structure that incorporates all elements of corporate governance, risk, and controls. This view is supported by Lyons (2011:8), thus highlighting the necessity for a corporate oversight framework to ensure that the interests of all stakeholders are safeguarded by the various lines of defence. Such a framework will reassure stakeholders that the organisation is fulfilling its fiduciary, regulatory, and legal obligations, while creating and sustaining long-term shareholder value (Lyons 2011:8).

Some authors, however, suggest that internal audit should coordinate the combined assurance efforts in organisations. Mihret and Admassu (2011:67) identify internal audit as the primary resource that should be used to manage the need for increased interaction between the four areas responsible for ensuring effective corporate governance, that is, between the board, management, internal audit and external audit. Daugherty and Anderson (2012:41) state that combined assurance provides internal audit with a unique opportunity to act as the assurance coordinator in the organisation, and that internal audit is a perfect candidate for this role, especially in the initial stages of combined assurance implementation. The role of assurance coordinator will consist of: identifying the assurance providers in the organisation; assigning the assurance providers to risks; assessing the reliance that can be placed on each assurance provider; analysing the areas where significant assurance gaps have been identified, and lastly, reporting to the governance structures (Daugherty & Anderson 2012: 41). Because internal audit has knowledge and experience of the organisation's governance structure, policies and frameworks, operational processes, risks and controls, it is therefore in the best position to drive the implementation of a combined assurance process (PWC 2010:11). Gramling *et al* (2004:196) warn, however, that the presence of appropriate skills and quality resources in the internal audit function are prerequisites for ensuring that this role can be fulfilled effectively in the organisation.

In the combined assurance process, taking on the coordinating role together with that of the third line of defence also implies a dual role for internal audit. Therefore, the roles assigned to internal audit should be carefully considered as they may affect their independence. For instance, internal audit should not take on any of the functions categorised under the first and second lines of defence (Christopher, Sarens & Leung 2009:203; De Zwaan, Stewart & Subramaniam 2011:587; IIA 2012:10; ECIIA 2012:6).

3.3 Critical success factors when implementing combined assurance

The third theme of discussion in the literature review revolves around the critical success factors when implementing combined assurance. It is clear that certain critical factors need to be present if combined assurance implementation is to be successful (PWC 2011:6; Sarens *et al* 2012:90-98; EY 2013:3). These factors can be broadly categorised as follows:

3.3.1 Proper risk management

Mature risk management processes should be present (Sarens *et al* 2012:90-98). These should ensure the provision of relevant and accurate risk information (PWC 2011:6), by following a standardised approach for identifying and compiling a key risk universe (EY 2013:3). Each risk has to have risk owners assigned to it (EY 2013:3). In addition, a common risk language and rating methodology needs to be agreed on (PWC 2011:6; Sarens *et al* 2012:90-98; EY 2013:3).

3.3.2 Leadership and buy-in from management

Sarens *et al (*2012:90-98) identify cultivating the correct "tone at the top", a strong culture of risk awareness, and executive management buy-in as critical success factors for combined assurance. Accordingly, the board or the audit committee should act as an executive sponsor for combined assurance and should determine, on the basis of the risk appetite and tolerance levels set by the board, the desired level of assurance needed (PWC 2011:6; EY 2013:3).

3.3.3 Proper planning and coordination

The effective planning and coordination of assurance activities are critical for implementing combined assurance successfully (KPMG 2012:16). In many organisations special assurance committees are being set up to drive and implement coordination between assurance providers, to enhance information sharing, and to monitor assurance activities effectively (KPMG 2012:16; Sarens *et al* 2012:97-98). KPMG has noted a strong correlation between satisfaction with assurance planning and coordination, and the existence of such an assurance committee (KPMG 2012:16).

The literature also points out some challenges with regard to the coordination of assurance services. KPMG (2012:6) remarks that the understanding of key risks, coordinated planning and joint audits between assurance providers is limited, and warns that, in a combined assurance approach, a lack of clear leadership and coordination between internal and external audit may result in redundancy and inefficiency (KPMG 2012:15). Sarens *et al* (2012:75) note the challenges faced by global organisations in coordinating the different assurance providers and explain that in global organisations various interfaces and additional points of coordination may be identified between assurance providers, thus increasing the difficulty of coordinating the activities.

Practise Advisory 2050-2: *Assurance maps* (IIA 2009) promotes assurance maps as a valuable tool for coordinating risk management and assurance activities, and enhancing the effectiveness of risk management efforts. Furthermore, assurance maps can identify duplication and overlaps in assurance activities related to key risks, assist in defining and limiting the scope of, and assigning roles and responsibilities to, the various assurance providers, and assist in identifying any gaps in assurance coverage.

3.3.4 Clarified roles and responsibilities

Roles and responsibilities need to be identified and agreed to between the assurance providers (Porter 2009:172; KPMG 2012:6). The amount of reliance that can be placed on the assurance provided should be assessed on the basis of the assurance providers' maturity level (IIA 2011:4; PWC 2011:6). Such maturity should be assessed annually, taking into account the skills and experience levels of the assurance provider, the scope and frequency of the assurance activities, the methodology applied, whether or not there are any conflicts of interest in the function, and whether there is an annual independent quality review of the function (PWC 2011:6).

Regular communication and interaction between the internal and external audit functions reinforces the strength of the combined assurance process (ECIIA 2012:6). Clear and open communication lines should exist between the various assurance providers and the stakeholders (Porter 2009:172; Sarens *et al* 2012: 90-98). Communication is not only essential for obtaining an understanding of the roles and responsibilities of the different assurance providers in providing assurance on key risks and objectives, but also assists in identifying duplications and omissions, thus ensuring adequate coverage of key risks (Sarens *et al* 2012:98).

4 RESEARCH FINDINGS AND INTERPRETATIONS

In the following sections, specific aspects of the state of combined assurance in the financial services industry in South Africa are discussed, based on the results of the empirical study and with reference to the literature review.

4.1 Introducing the concept of combined assurance and clarifying its purpose in organisations

Respondents were asked to indicate whether their organisations had introduced any combined assurance practices, and if so, when they had commenced with the implementation of combined assurance in their organisations. What is remarkable here is that the majority of companies (five of the eight surveyed) commenced with the implementation of combined assurance between 2009 and 2010 – the two-year period immediately after King III had introduced combined assurance as a principle of corporate governance in South Africa. A sixth company started with implementation in 2012. This, and the fact that listed companies are compelled to either comply with King III recommendations or to explain why they don't (IOD 2013:2), emphasises the importance of governance and reporting regulations, and the value placed on such regulations by leading organisations in South Africa. A more cynical interpretation of the response may be that organisations obey such regulations for the sake of compliance, without considering the value that may be derived from such compliance. One response indicated that the company had started with the implementation of combined assurance prior to the release of King III. In the follow-up interview, this respondent revealed the perception that the practice of combined assurance in its simplest form includes cooperation between internal and external audit, a situation that has existed prior to the publication of King III.

Although all the respondents indicated that their companies had started with the implementation of combined assurance, the follow-up interviews revealed that most are still on the way to the full implementation required in terms of King III. One of the responses indicated that the company is about a year away from full implementation and compliance with King III. During the interviews one of the respondents remarked that "*the implementation of combined assurance is seen as a journey*". Another commented that "*combined assurance should be seen as a philosophy rather than a methodology*", and explained that their organisation had put a lot of effort into formalising the philosophy in terms of a methodology with frameworks and standards, without deriving real value from the process. This resulted in a divergence of effort in that their combined assurance process eventually focused on inherent risk, while the organisation's management focused on residual risk.

One respondent commented that, although management believed that combined assurance had been implemented, the process was still immature as it lacked formalisation through combined assurance charters, frameworks, and the formalisation of roles and responsibilities. Another interviewee also expressed concerns about the immaturity of combined assurance in their company, owing to it being limited mainly to the interaction between internal and external audit, without any interaction being extended to the other assurance providers.

Respondents were requested to indicate any global affiliation, and to state whether or not the primary listing of their company was on the JSE. The responses to these questions, combined with the responses discussed above, indicate a positive correlation between the primary listing of the organisation and the progress made with the implementation of combined assurance. One of the eight companies selected for the survey had not commenced with the implementation of combined assurance as it had its primary listing on a foreign stock exchange, where adherence to King III is not required. Hence, this company did not complete the questionnaire. All the other companies that indicated global affiliations also indicated that they had already started with the implementation of combined assurance.

One of the difficulties for global organisations is that the concept of combined assurance has not been introduced elsewhere in the world. The fact that combined assurance has not found its way onto the international scene was raised by one respondent as a concern. This respondent referred particularly to recommendations by the Committee on Internal Audit Guidance for Finance Services in the United Kingdom (Chartered Institute of Internal Auditors 2013:12), which the respondent perceived to be in direct conflict with the combined assurance approach practised in South African organisations, and who expressed the view that "*if not accepted internationally, the practice of combined assurance may become difficult to sustain in South Africa*".

Companies that indicated global affiliation other than a primary JSE listing (that is, companies with global parent companies and/or subsidiaries) nevertheless responded positively with regard to the effect that combined assurance has had on their international ties, commenting that through their efforts combined assurance had been recommended to their international holding companies, where the value has been noticed by global investors. Similarly, some African subsidiaries of organisations interviewed had realised the benefits associated with combined assurance and had also started implementing it voluntarily in their organisations. One respondent perceived the most significant contributions their combined assurance efforts had made to their African subsidiaries to be the enhancing of the process of risk identification and encouraging a holistic view of risk.

4.2 Roles and responsibilities in the combined assurance process

From the literature review it is evident that a coordinated and combined approach is necessary for the effective implementation of combined assurance. This approach demands that all the parties involved should realise the importance of their respective roles in the process.

Stakeholders

Responses confirmed the importance of adequate buy-in from the key stakeholders. Six of the seven respondents (85.7%) regarded buy-in from key stakeholders and the audit committee chairman, as well as executive management setting the "tone at the top", to be extremely important foundational areas for the successful implementation of combined assurance (see Table 5).

The importance of the buy-in of the audit committee chairman (and his/her focus on the process) for the successful implementation of combined assurance was further emphasised during the interviews. One CAE interviewed mentioned that their organisation was struggling to implement combined assurance effectively, with the lack of an executive sponsor being highlighted as one of the main barriers.

As emphasised by the literature review, the audit committee is one of the primary stakeholders of combined assurance and it is therefore vital for it to be involved. Two of the questions included in the questionnaire prompted reflection on this issue. In response to one of the questions, all respondents indicated that their audit committees receive a report on long-outstanding audit findings, including the management actions taken to address them, and that these are then actively monitored by the audit committee. The responses to the other question indicated that, in the majority of companies surveyed (85.7%), the timeous implementation of combined assurance actions and findings is actively monitored by executive management.

Respondents were required to indicate whether or not the audit committees play an active role in combined assurance. The response to this question is reflected in Table 2. In five of the companies surveyed (71.42%) the audit committee played an active role in overseeing combined assurance efforts in the company.

Table 2: Responses to Question 7 of the questionnaire

Active role played by audit committee in combined assurance	Number	%
Yes	5	71.42
No	1	14.29
Not answered	1	14.29
	7	**100.00**

Another question required respondents to indicate the proportion of agenda time audit committees spend on assurance matters. An analysis of the responses to this question indicated that, on average, the audit committees spend about 8.81% of overall agenda time on combined assurance matters. Internal audit takes up the greatest allocation of agenda time (22.37%), followed by financial analysis (21.19%), external audit (15.59%), and then regulatory risk management (11.57%) (see Table 3).

Further analysis of these responses was performed, comparing those companies that responded that the audit committee is perceived to play an active role in combined assurance to those companies that did not respond affirmatively to this question. Interestingly, this analysis points out that, for companies where the audit committee plays an active role in combined assurance, the agenda time of audit committee meetings is more evenly spread between the various topics dealing with different assurance providers, as opposed to companies where the audit committee does not play an active role in combined assurance. For the latter, more than half (55.26%) of the agenda time is spent on internal audit and external audit, as opposed to a third (29.75%) of the agenda time spent where the audit committees are reported to play an active role (see Table 3).

Table 3 clearly illustrates the difference in the time allocated to the various aspects of combined assurance on the agenda of audit committee meetings, where audit committees play either an active or an inactive role in combined assurance.

Table 3: Analysis of responses to Questions 7 and 8 of the questionnaire

Aspects of combined assurance in the agenda of audit committee meetings	% of time allocated (all companies included in the survey)	% of time allocated (audit committee plays an active role)	% of time allocated (audit committee does not play an active role)
Regulatory Risk	11.57	12.06	10.53
Information Governance	7.33	8.31	5.26
Internal Audit	22.37	15.50	36.84
External audit	15.59	14.25	18.42
Combined Assurance	8.81	10.50	5.26
Financial Analysis	21.19	23.75	15.79
Social and Environmental	3.24	4.78	0.00
Governance	6.95	6.50	7.89
Other	2.95	4.35	0.00
	100.00	**100.00**	**100.00**

Assurance providers

Respondents were required to identify the role players in combined assurance and to allocate them to the first, second, or third line of defence. All of the companies surveyed indicated the presence of information technology (IT) risk management, internal audit, and external audit as assurance providers in their combined assurance process. In addition, management, enterprise risk management, regulatory risk management, and legal departments were identified as assurance providers in six of the organisations (85.7%). It is interesting to note that the legal department was seen by some organisations as an assurance provider in the first line of defence and by others as a second-line defence assurance provider. Only one of the respondents (14.3%) considered the ethics department, regulators, quality control, health and safety officers, and rating agencies to be assurance providers.

Coordinators

The literature review indicated that the audit committee and the internal audit function are the most popular nominations for a champion for the combined assurance process. In the survey, respondents were requested to indicate who chairs the combined assurance forum or committee in their organisation. In the majority of organisations surveyed, internal audit, through the CAE, performed this role of combined assurance champion. It is interesting to note the exceptions in two organisations: in one this role is performed by the chief risk officer, and in the other by the corporate governance function. Nevertheless, internal audit did assist the chief risk officer in defining and identifying the various assurance providers, and in formulating and drafting the assurance frameworks and standards. None of the respondents identified the audit committee as the combined assurance champion. Probing the role of internal audit as a champion of the combined assurance process during the interviews revealed that this role has significantly elevated the profile of internal audit. One of the respondents commented that the chief executive officer, in recognising the specific role internal audit had played in the implementation of combined assurance, had realised the power that can be created from the alignment of the three lines of defence.

4.3 Critical success factors in the implementation of combined assurance

Three questions were used to shed light on the critical success factors for combined assurance implementation.

The first question (question 9 of the survey) identified sixteen initiatives that have been associated with combined assurance in the literature (see Table 4). Respondents were asked to rate the level of implementation of each of these aspects in their organisations according to a rating scale where 1 represents that the initiative has been implemented, 2 represents implementation within the next 12 months, 3 represents implementation within the next 24 months and 4 represents that the initiative is not considered for implementation in the near future.

Two organisations responded that their organisations had already implemented thirteen of the initiatives and that they intended to implement the remaining three within the next 12 to 24 months. One of the organisations had implemented ten of the initiatives and was not considering implementing any of the others. Three organisations had implemented fewer than half of the initiatives, while one of the organisations had not implemented any of the initiatives, but indicated that the organisation intended to implement thirteen of the initiatives over the next 24 months.

The initiatives implemented by most organisations, as shown in Table 4, were 1, 4, 7, 8, and 14. In addition to those initiatives, all organisations intended to have implemented initiatives 3 and 11 within 24 months (see Table 4). The initiatives least frequently implemented were 5 and 12 (implemented by only one organisation). Three respondents (43%) indicated that joint audits between different assurance providers had not been considered by their organisations (initiative 15 in Table 4).

Table 4: List of possible initiatives to be implemented in the combined assurance process, used in Question 9 of the questionnaire

Combined assurance initiatives	
1	Establishing a combined assurance framework
2	Establishing a combined assurance charter
3	Developing specific agreements between all assurance providers on their respective roles and responsibilities
4	Creating a common risk language
5	Implementing an Enterprise Governance Risk and Compliance (GRC) platform to manage risk throughout the organisation
6	Performing integrated risk assessments with the input of all assurance providers
7	Creating a risk coverage map, linking risks to processes and controls
8	Linking risk coverage maps to control owners (assurance maps)
9	Linking risk coverage maps to internal and external audit assurance provided on key risks
10	Creating and conducting maturity assessments for assessing assurance provider maturity
11	Providing the audit committee with a combined assurance report
12	Using an aligned, coordinated and standardised reporting format that is used by all combined assurance providers
13	Presenting consolidated combined assurance results to the audit committee
14	Using combined risk assessments/maps to inform the annual internal audit plan
15	Internal audit conducting joint audits with other assurance providers
16	Creating a combined assurance forum/committee to coordinate combined assurance

The second question (survey question 13) used a Likert-type scale approach to assess the importance of fourteen foundational areas in ensuring the effectiveness of combined assurance. For each of the areas, respondents had to rate its significance as being not important (1), somewhat important (2), important (3), very important (4), or extremely important (5). Analysis of the responses to this question indicated that executive management setting the “tone at the top”, buy-in from key stakeholders, and buy-in from the chairman of the audit committee were considered to be the most important foundational areas in ensuring the effectiveness of combined assurance. This was followed by a strong risk culture across the company, effective corporate governance structures, and buy-in from the audit committee. Performance reward systems, formalised and documented policies and procedures, and having employees sign a code of conduct were rated least important (see Table 5).

Table 5: Importance of the foundational items for effective combined assurance (response to Question 13 of the questionnaire)

Foundational areas to ensure the effectiveness of combined assurance	Average weighting, taking into account all responses
Executive management setting the ‘tone at the top’	4.86
Buy-in from key stakeholders	4.86
Buy-in from chairman of the audit committee	4.86
Effective corporate governance structures	4.71
Strong risk culture across the company	4.71
Buy in from audit committee	4.57
Risk appetite – clear definition and communicated throughout the company	4.43
Strong organisational culture across the company	4.43
Board training on combined assurance	4.14
Uniform risk language and rating methodology across the company	4.14
Buy in from chairman of the board	4.14
Performance reward systems linked to effective risk management	4.00
Formalised, documented and updated policies and procedures	3.57
Code of conduct signed by all employees in the company	3.43

The third question shedding light on critical success factors (survey question 15) identified nine critical success factors from the literature and requested respondents to select the five most critical factors that needed to be present to ensure the effective implementation of combined assurance (see Table 6). Although responses varied significantly, *combined assurance champion* received the most 'first' ratings, while *a combined assurance framework and methodology* received the second-most 'first' ratings, and was also the factor rated by the highest number of respondents. Although not awarded any first ratings, *evaluation of assurance provided* was also rated by six of the respondents (85.7%).

Table 6: Critical success factors for the successful implementation of combined assurance (used in Question 15 of the questionnaire)

Critical success factors
Executive sponsor
Combined assurance champion
Mature risk management function
Defined risk appetite and tolerance
Combined assurance framework and methodology
Common risk language
GRC platform
Communication and training on combined assurance throughout the company
Evaluating the quality and effectiveness of assurance provided by the various assurance providers

The literature review identified four broad categories in the discussion of the critical success factors for combined assurance implementation. The results of the empirical study revealed the following with regard to each category:

Proper risk management

During the follow-up interviews with the CAEs, the adequacy and effectiveness of a risk management function was highlighted as a critical success factor. One of the respondents commented during the interview that *"combined assurance can only be as strong as the risk management foundation"*. The interviews further revealed that a contributing factor to the immaturity of combined assurance at one company was the lack of an effective and mature risk management function, including the absence of a common risk taxonomy, risk frameworks and standards.

However, it is interesting to note that the maturity of the risk management function was only rated as critical by one of the companies (see Table 6). This is in direct contrast to the responses received from the CAEs during the interviews, where the lack of a mature risk management function was highlighted as one of the challenges for the successful implementation of combined assurance by several of the respondents.

Another challenge experienced by one of the companies related to getting the first line of defence to understand its roles and responsibilities as risk owners. The respondent commented that management, as the first line of defence, needs to understand that they own and manage risk and are ultimately accountable for that risk and that the second line is there only to assist in managing those risks. The respondent further remarked that in their organisation this shift in focus was "*a massive process that needs to be driven from the top*". In another organisation the separation of the risk management function between the first and second lines of defence was said to be blurred. This had resulted in conflicting duties for risk management, as they might be seen to be fulfilling management responsibilities, which affected the maturity of the function and ultimately the reliance placed on them by the third line of defence.

Leadership and buy-in from management

The response to survey Question 13 highlights the importance of leadership and buy-in from management in ensuring the effective implementation of combined assurance. Six of the seven CAEs regarded buy-in from key stakeholders and the chairman of the audit committee as being extremely important foundational areas for effective combined assurance (see Table 5). In addition, executive management setting the "tone at the top" was identified as the most critical foundational factor by six of the seven CAEs.

The follow-up interviews revealed that a lack of buy-in from the audit committee chairman, together with the insufficient maturity of assurance providers, were the most important factors preventing one of the organisations from implementing effective combined assurance. Another organisation interviewed was struggling to implement combined assurance effectively and the lack of an executive sponsor was highlighted as one of their main barriers. A third respondent commented that the main challenge faced by their organisation related to obtaining management buy-in. This respondent commented that, in order to obtain executive buy-in, the value proposition had to be effectively communicated to management.

Proper planning and coordination

The significance of proper planning and coordination in combined assurance is indicated by the response to Question 15, where two-thirds of respondents (or 5 companies) indicated the presence of a combined assurance champion as the most important success factor, and three of the respondents perceived a combined assurance framework and methodology to be a critical success factor (see Table 6). Only two of the companies surveyed had progressed to the point where they had appointed a specific forum or committee to coordinate combined assurance. In one company, this committee was chaired by the CAE, while in the other it was chaired by the head of operational risk management. In response to Question 9, all respondents indicated their organisation's intention to implement a coordinating committee within the next 12 to 24 months; this emphasises the importance of coordinating the combined assurance process properly. Some CAEs indicated in the interviews that this coordinating committee would form part of the current governance committees, so as to avoid the establishment of yet more committees and forums.

With regard to the planning of combined assurance efforts, assurance maps seem to be a commonly accepted tool. All of the respondents indicated in response to Question 9 that their organisations were using, or were intending to use, assurance maps and/or risk coverage maps in the near future to link risks to processes and controls, and to link risk coverage maps to control owners. All respondents indicated that combined risk maps are used to inform the annual internal audit plan, or that they intend using them in the near future to do so.

Clarified roles and responsibilities

In response to Question 9 (see Table 4), only three of the organisations surveyed indicated that they had established a separate charter for combined assurance. One of these respondents commented that establishing a combined assurance charter is a challenge, as the roles and responsibilities of the different assurance providers first need to be established. Two other organisations indicated that they were not considering establishing a separate charter for combined assurance.

Nevertheless, all respondents indicated that they had drawn up, or intended to draw up, specific agreements between all assurance providers recording their respective roles and responsibilities. Further discussion during the interviews revealed that there were still some areas of duplication of assurance activities and that the first line of defence was still experiencing audit fatigue. One respondent commented that *"due to the different assurance providers belonging to different institutions and having to abide by different standards there will be some duplication and you will not be able to eradicate duplication completely".*

One organisation commented that the biggest challenge was for the different assurance providers to value each other's work. This was mainly as a result of the immaturity of the assurance functions within the three lines of defence, thus resulting in a lack of trust in the quality of work produced by the assurance providers which, in turn, affected the reliance placed on the work performed.

One of the respondents commented that the sharing of assurance results between the assurance providers could be improved because in their company not all assurance reports were yet shared. Another respondent raised the reluctance on the part of external audit to share detailed scope documents and working papers as an issue that was hampering reliance decisions from other assurance providers, especially internal audit, resulting in the reduced leveraging of external audit's work. On the question of why it is so difficult for different assurance functions to work together, one CAE commented that *"it is about a loss of control because you don't have distinct lines anymore, you have people working together to enhance the control environment. It probably becomes an insecurity matter or that they are worried that their inadequacies might be revealed with this type of approach. The purpose is as a collective to enhance the control fabric of the organisation"*.

5 CONCLUSION

This article presented the findings of a study conducted to establish the status of combined assurance implementation in organisations in the financial services industry in South Africa. The study followed a mixed method approach which consisted of a literature review and an empirical study comprising a survey and structured interviews. The companies surveyed represent 71% of the market capitalisation of companies in the banks, life insurance, and general finance sectors of the JSE, and the survey obtained the responses of the CAEs in those organisations.

The study found that most organisations in the financial services industry in South Africa had started implementing combined assurance practices as required by King III, and noted that such implementation had commenced in the two years following the publication of the King III report. Implementation is, however, a journey and organisations are still at various levels of maturity in terms of their stages of implementation of combined assurance practices. Many organisations are still struggling with various barriers to effective implementation; these include a lack of buy-in by executive management and the audit committee, immature second-line risk management functions, different regulatory environments for JSE-listed and foreign-listed companies, the lack of a combined assurance champion within the organisation, and limited sharing of scope documents and working papers by external audit. Implementing a GRC platform in the organisation to ensure that there is just one view of the risk environment is currently not a priority in most organisations.

The study further found that organisations with primary listings outside South Africa, or with dual listings, have not yet completely implemented combined assurance, owing to the different regulatory requirements in their "other" countries.

The study identified certain fundamental and key areas that are important for ensuring that combined assurance is successfully implemented in an organisation. It was accordingly found that the identification (and appointment) of a combined assurance champion is a critical success factor for combined assurance. This champion should be supported by an executive sponsor, which ideally should be the chief executive officer. Organisations should furthermore ensure that the first and second lines of defence functions are mature in their risk management practices. Moreover, the roles and responsibilities of the various assurance providers should be formalised in a combined assurance framework. Buy-in and active participation by the chairman of the audit committee and the audit committee as a whole is also vital for combined assurance. In organisations where the audit committee plays an active role in combined assurance, it was found that the focus at audit committee meetings was broader, with the audit committee's agenda time more evenly shared across all assurance providers.

In the organisation, the internal audit function, through the CAE, is in an ideal position to perform the role of combined assurance champion because internal audit has a holistic view of the risk and control environment in the organisation. Most of the organisations surveyed indicated that the CAE does indeed play the role of combined assurance champion in the organisation. If this role is undertaken successfully, it is believed that this improves the stature of internal audit in the organisation. However, in this role the internal audit function should take care not to take on operational risk management duties. Thus, a clear understanding of the role and responsibility of internal audit, as a third line of defence, is also critical in ensuring that the lines between its various roles and responsibilities do not become blurred.

6 RECOMMENDATIONS FOR FUTURE RESEARCH

Further studies could expand on the views and perceptions of additional role players, other than the CAEs, in the three lines of defence. Studies could also expand on the current state of combined assurance practices of organisations listed on the JSE in sectors other than the financial services industry.

The impact that a foreign primary listing or dual listing has for South African companies on the implementation of combined assurance could also be studied further. Finally, the benefits of combined assurance could be articulated and used by combined assurance advocates to obtain stakeholder buy-in and to serve as a motivation for the implementation of combined assurance in more organisations.

REFERENCES

Bank for International Settlement. 2011. *Principles for the sound management of operational risk.* [Online]. http://www.bis.org/publ/bcbs195.pdf (Accesed: 2 May 2013).

Beeld. 2014. JSE Ltd Closing price 2014/09/12. *Beeld*, 13 September:15.

BIS, see Bank for International Settlement.

Brody, R.G., Golen, S.P. & Reckers, P.M.J. 1998. An empirical investigation of the interface between internal and external auditors. *Accounting and Business Research*, 28(3):161-171.

Chartered Institute of Internal Auditors. 2013. *Effective internal audit in the financial services sector.* [Online]. http://www.iia.org.uk/media/354788/0758_effective_internal_audit_financial_webfinal.pdf (Accessed: 14 September 2014).

Christopher, J., Sarens, G. & Leung, P. 2009. A critical analysis of the independence of the internal audit function: evidence from Australia. *Accounting, Auditing & Accountability Journal*, 22(2):200-220.

Corporate Executive Board. 2013. *Introduction to integrated assurance* [Online]. https://audit.executiveboard.com/Members/ResearchAndTools/Abstract.aspx?cid=101206565&fs=1&q=integrated+assurance&program=&ds=1 (Accessed: 19 August 2014).

Creswell, J.W. 2009. *Research Design. Qualitative, quantitative and mixed methods approaches.* 3rd edition. USA: SAGE Publications Ltd.

Daugherty, B. & Anderson, U. 2012. The third line of defense: internal audit's role in the governance process. *Internal Auditing*, 27(4):38-41.

De Zwaan, L., Stewart, J. & Subramaniam, N. 2011. Internal audit involvement in enterprise risk management. *Managerial Auditing Journal*, 26(7):586-604.

Deloitte. 2012. *Value add through combined assurance*. [Online]. http://www.iiasa.org.za/Regions/Namibia/Presentations/Value_Add_Combined_Assurance.pdf (Accessed: 1 May 2013).

ECIIA, see European Confederation of Institutes of Internal Audit.

European Confederation of Institutes of Internal Audit (ECIIA). 2012. *Corporate Governance insights.* [Online]. http://ec.europa.eu/internal_market/consultations/2012/banking_sector/registered-organisations/eciia-annex_en.pdf (Accessed: 3 August 2014).

European Confederation of Institutes of Internal Audit (ECIIA) and Federation of European Risk Management Associations (FERMA). 2010. *Guidance on the 8th Company Law Directive. Article 41.* [Online]. http://www.theiia.org/chapters/pubdocs/303/eciia_ferma_guidance_on_the_8th_eu_company_law_directive_part_2.pdf (Accessed: 3 August 2014).

EY. 2013. *Maximising value from your lines of defense*. [Online]. http://www.ey.com/Publication/vwLUAssets/EY-Maximizing-value-from-your-lines-of-defense/$File/EY-Maximizing-value-from-your-lines-of-defense.pdf (Accessed: 20 July 2014).

Felix, W.L., Audrey, A., Gramling, A.A. & Maletta, M.J. 2001. The contribution of internal audit as a determinant of external audit fees and factors influencing this contribution. *Journal of Accounting Research*, 39(3):513-534.

FERMA, see Federation of European Risk Management Associations.

Fraser, I. & Henry, W. 2007. Embedding risk management: structures and approaches. *Managerial Auditing Journal*, 22(4):392-409.

Gramling, A.A., Maletta, M.J., Schneider, A. & Church, B.K. 2004. The role of the internal audit function in corporate governance: a synthesis of the extant internal auditing literature and directions for future research. *Journal of Accounting Literature*, 2004(23):194-244.

Institute of Directors (IOD) Southern Africa. 2009. *King Code of Governance for South Africa*. South Africa.

Institute of Directors (IOD) Southern Africa. 2013. *Practise notes: King III reporting in terms of the JSE listing requirements.* South Africa.

IOD, see Institute of Directors.

IIA, see Institute for Internal Auditors.

Institute of Internal Auditors (IIA). 2009. *International Professional Practises Framework.* The Institute of Internal Auditors. Altamonte. USA.

Institute of Internal Auditors (IIA). 2011. *Reliance by internal audit on other assurance providers*. The Institute of Internal Auditors. Altamonte. USA.

Institute of Internal Auditors (IIA). 2012. *Coordinating risk management and assurance*. The Institute of Internal Auditors. Altamonte. USA.

Institute of Internal Auditors (IIA). 2013. *The three lines of defense in effective risk management and control.* The Institute of Internal Auditors. Altamonte. USA.

IAASB, see International Auditing and Assurance Standards Board.

International Auditing and Assurance Standards Board (IAASB). 2013. *Handbook of International Quality Control, Auditing Review, Other Assurance, and Related Services Pronouncements*. International Federation of Accountants (IFAC). New York. USA.

KPMG. 2012. *Effective assurance.* [Online]. https://www.kpmg.com/CH/en/Library/Articles-Publications/Documents/Audit/pub-20120524-effektive-assurance-en.pdf (Accessed: 3 August 2014).

Lyons, S. 2011. *Corporate oversight and stakeholder lines of defense.* [Online]. http://ssrn.com/abstract=1938360 (Accessed: 20 July 2014).

Mihret, D.G. & Admassu, M.A. 2011. Reliance of external auditors on internal audit work: a corporate governance perspective. *International Business Research*, 4(2):67-79.

Munro, L. & Stewart, J. 2010. External auditors' reliance on internal auditing: further evidence. *Managerial Auditing Journal*, 26(6):464-481.

Porter, B.A. 2009. The audit trinity: the key to securing corporate accountability. *Managerial Auditing Journal*, 24(2):156-182.

PriceWaterhouseCoopers. 2010. *Implementing a combined assurance approach in the era of King III.* [Online]. https://www.pwc.co.za/en/assets/pdf/SteeringPoint-KingIII-Combined-Assurance-11.pdf (Accessed: 19 August 2014).

PriceWaterhouseCoopers. 2011. *Moving forward with combined assurance*. [Online] http://www.imfo.co.za/presentations/Moving%20forward%20with%20combined%20assurance.ppt (Accessed: 6 May 2013).

PriceWaterhouseCoopers. 2013. *Combined assurance practical approach and reporting key learning's.* [Online]. http://oag.treasury.gov.za/Event%20Documentation/20130228%20Public%20Entities%20Risk%20Management%20Forum/2.%20System%20of%20Combined%20Assurance%20and%20Institutional%20performance%20-%20A%20Moosa%20and%20JC%20Heyns.pdf (Accessed: 1 May 2013).

PWC, see PriceWaterhouseCoopers.

Roos, M. 2012. Audit committees and combined assurance. *Auditing SA,* Summer 2011/12:31-34.

Sarens, G. & De Beelde, I. 2006. Internal auditors' perception about their role in risk management: a comparison between US and Belgian companies. *Managerial Auditing Journal*, 21(1):63-80.

Sarens, G., Decaux, L. & Lenz, R. 2012. *Combined Assurance: case studies on a holistic approach to organizational governance*. The Institute of Internal Auditors Research Foundation. Altamonte. USA.

Schneider, A. 2009. The nature, impact and facilitation of external auditor reliance on internal auditing. *Academy of Accounting and Financial Studies Journal*, 13(4):41-53.

Spira, L.F. & Page, M. 2003. Risk management: the reinvention of internal control and the changing role of internal audit. *Accounting, Auditing and Accountability Journal*, 16(4):640-661.

Tapestry Networks. 2004. *The internal auditor's perspective.* [Online]. http://www.tapestrynetworks.com/documents/Tapestry_EY_ACLN_July04_InSights.pdf. (Accessed: 9 August 2014).

Turlea, E., Mocanu, M. & Radu, C. 2010. Corporate governance in the banking industry. *Accounting and Management Information Systems*, 9(3):379-402.

SOUTHERN AFRICAN JOURNAL
OF ACCOUNTABILITY AND
AUDITING RESEARCH

The Editor
*Southern African Journal of Accountability
and Auditing Research (SAJAAR)*
P O Box 36303
Menlo Park 0102
South Africa

Editorial requirements

Version 13/05/2015

A General

The *Southern African Journal of Accountability and Auditing Research* (SAJAAR) is the research journal of the Southern African Institute of Government Auditors (SAIGA).

The Southern African Institute of Government Auditors is an independent Institute which aims to advance accountability and auditing in particular.

The publication of a fully accredited scientific journal in South Africa is one of SAIGA's contributions towards advancing accountability and auditing in our country. It is also designed to assist in the professionalisation of auditors and government auditors in particular. The Institute's premise is that uncensored scholarly debate will contribute towards the development of the disciplines that strengthen accountability and auditing in particular. SAIGA endeavors to ensure that important accountability concepts and the external audit function in particular, are not marginalised.

B Accreditation of the journal (SAJAAR)

The *Southern African Journal of Accountability and Auditing Research* is accredited by the South African Department of Higher Education and Training as a research journal and contributions (articles) qualify for subsidies which the Department of Higher Education and Training grants to tertiary institutions in this regard.

C Fields of interest covered

With this scientific journal it is intended to provide a wide coverage of the issues that are subject to scholarly debate around accountability and auditing preferably with emphasis and focus on the public sector. The topics and debate should consequently be directed at *accountability* and *auditing in the public sector*, albeit in a broad context. Research projects directed at accountancy or the education of *accountants* fall outside the intended scope, unless a direct relation is established and identified between the phenomenon under investigation and either *auditing* or *accountability*. Internal auditing is also not the main focus of this journal, unless a public sector perspective is linked to the internal auditing research topic. Preference will be given to contributions that address *accountability* and *auditing* elements and topics directly in a public sector context.

Opportunities to publish scholarly work focusing on the broader accountability framework are limited and related research findings have to compete with material submitted for publishing on subjects such as Economics, Management and Accounting in existing South African journals. The establishment of a research journal focusing on accountability and auditing (with a focus on the public sector) therefore heralds a new age for these key disciplines in Southern Africa. It is also an attempt to ensure that the public sector is not marginalised.

D Sequence of publication

The *Southern African Journal of Accountability and Auditing Research* is published annually.
Should sufficient acceptable manuscripts be received to warrant more than one issue, SAIGA will consider publishing more than one issue per year.

The normal publication date is towards the end of a calendar year.

E SAJAAR readership

Every issue of *SAJAAR* is distributed to a wide audience:

- South African legal deposit libraries
- libraries of South African tertiary institutions
- other major South African libraries
- libraries of professional bodies in South Africa
- selected staff from the Auditor-General South Africa
- other senior role players in South Africa's public sector
- subscribers (individuals and entities).

F Authors' responsibilities

The submission of an article for publication in *SAJAAR* activates a reviewing process that involves expert knowledge and linguistic editors. Although the Institute levies certain charges (for example page fees) this only covers a small percentage of the publication and distribution costs. It is therefore important that authors realise that the editorial requirements set out below are designed to create an effective, efficient and economical reviewing and publishing process. Strict adherence to these basic requirements is therefore essential.

G Fees payable

The following fees are payable at various stages of the process (authors should note that no new manuscripts may be submitted for review and publishing, if any fees, relating to previously published articles by the author/(s) are still outstanding):

South African contributors:

Page fees: of R313.50 per page (R275 plus 14% VAT) [page refers to the actual numbered pages as contained in the published journal] are payable as a condition for the final acceptance of articles (fee valid for 2015). The above fees are subject to a 10% annual increase. The Editor will issue a single invoice to the "representative author" (see definition below), which has to be paid before publication of the journal.

Linguistic editing fees: For every 10 pages (or part thereof) of the original, double spaced manuscript submitted, a fixed fee is payable. This fee is set as follows: 2015: R752.40 (R660 plus 14% VAT). The above fees are subject to a 10% annual increase. The Institute reserves the right to increase this amount, therefore authors are advised to consult the Institute's website for the latest fees. The linguistic fees are calculated based on the number of pages of the manuscript was submitted originally (typed in double spacing).

Administrative fees: Incomplete submissions create unnecessary work and result in additional correspondence and costs. Each time the SAIGA Secretariat has to refer a submission back to the author/(s) based on the non-compliance with the submission requirements, a standard charge of R438.90 (R385 plus 14% VAT) per communication is levied. This amount has to be paid before the article is published. The above fees are subject to a 10% annual increase.

Non-South African contributors*:*

Page fees: 75 US Dollars per manuscript page.
Linguistic editing fees: For every 10 pages: 160 US Dollars.
Administrative fees: 105 US Dollars per communication.
The above fees are subject to a 10% annual increase.

H The reviewing and publishing process

(a) Upon receipt of a submission, the SAIGA Secretariat checks the completeness of the submission and adherence to the editorial requirements as well as topic relevance and communicates with the authors(s) in this regard.

(b) Once the submission is complete and the editorial requirements adhered to, the article is entered into the reviewing process. From this point onward, the author(s) are not allowed to withdraw the article and SAIGA has the right to publish it.

(c) The Editor will provide the author(s) with feed-back from the members of the Editorial Board, suggestions to improve the article and necessary changes to get the article in a format for publishing.

(d) The Institute, through SAJAAR's Editor, may inform the author(s) that the article cannot be published and allow the author(s) to withdraw the article.

(e) Should the Editor decide that the article is publishable if the necessary changes are made and suggestions for improvement are affected, the article will then be sent for linguistic editing and improvements made.

(f) The author(s) then have to pay the linguistic fees and any administration fees that may have incurred. A single invoice will be made out to the "representative author" who has to fax a copy of the deposit slip as proof of payment to the SAIGA Secretariat.

(g) Based on the outcome of the linguistic process, the response to the reviewers' feed-back and other communications, the Editor will inform the author(s) of the acceptance of the article for publication or other conditions that have to be met before publication.

(h) The full page fees are then payable. A single invoice will be made out to the "representative author" who has to fax a copy of the deposit slip as proof of payment to the SAIGA Secretariat.

(i) All outstanding fees (linguistic and page fees) have to be paid within a month from the date of the invoice and proof of payment presented to the Institute. The journal will then be printed and published, including the articles of all authors whose fees have been paid. Articles related to unpaid fees will not be published in the current edition, but in the following edition.

(j) The "representative author" has to note that the payment of the invoice is his/her responsibility and that the "representative author" has to fax proof of payment to the SAIGA Secretariat. Where authors submit their invoices to their employers (e.g. universities) for payment, this does not involve SAIGA and it remains the responsibility of the "representative author" to pay the invoices and to provide the SAIGA Secretariat with the proof of payment. SAIGA will not follow up invoices with any employer or firm, but will only deal with the "representative author".

(k) Please also note that no article for publication in future issues of SAJAAR will be accepted if any of the authors of such an article has any fees outstanding.

(l) The author(s) will be informed of the publication of the journal and their copies sent to them.

I Elements of the submission

A submission consists of the following four elements:

1 The covering letter by the authors (pdf format)
2 The information sheet (pdf format)
3 The actual manuscript (MS WORD & pdf format)
4 The signed declaration (pdf format).

Details regarding the above requirements are set out below.

1 The covering letter by the authors (containing normal communications)

This letter is addressed to the Editor of SAJAAR and written on the letterhead of the author/(s) and signed by at least one person. It will contain the normal communications and no specific requirements as to the contents thereof are set.

The covering letter must be submitted as a pdf file and the file name must be constructed as follows: Surname of author – Covering Letter – date of submission (yyyy-mm-dd).
For example: *Smith – Covering Letter – 2014-04-14*.

2 The information sheet

A typed page (in a separate file) on which the following information must be provided:

2.1 the full title of the article
2.2 the full name(s) and surnames of the author(s)
2.3 the title(s) of the author(s)
2.4 their academic status
2.5 their current place of employment
2.6 the name of the institution (for example University) that needs to be disclosed next to their name (for purposes of accreditation of refereed articles)
2.7 the name of the “representative author”, the person who will be responsible for receiving and answering any correspondence and who will be responsible to pay the linguistic and page fees (only two invoices will be made out: one for the linguistic fees and one for the page fees)
2.8 postal address to which all correspondence may be sent (one elected representative address in the case of multiple authors)
2.9 e-mail address (one elected “representative author” and his/her address in the case of multiple authors)
2.10 contact telephone and fax numbers of the “representative author”
2.11 the details to whom the invoice(s) must be made out and a VAT registration number if available
2.12 a list of key words for cataloguing purposes.

The information sheet must be submitted as a pdf file and the file name must be constructed as follows: Surname of author – Information Sheet – date of submission (yyyy-mm-dd).
For example: *Smith – Information Sheet – 2014-04-14*.

3 The actual manuscript

The manuscript submitted for consideration must adhere to the following *technical standards*:

3.1 Be typed in Microsoft WORD in *double spacing* and paginated. All submissions must be prepared using MS WORD. Conversions from other word processing packages are not acceptable.
3.2 Be typed in the Arial font with an 11 point spacing (this applies to both main text and any endnotes that may be used).

3.3 Be free of any footers or headers or other graphics, lines and blocks sometimes used to enhance documents (blocks around each page, etc.).

3.4 Have a first page on which only the title of the article is printed together with an abstract (approximately 100 words) of the article (no names of authors on this page).

3.5 Be typed in such way that the names of the author/(s) do not appear in the actual manuscript (this does not apply to their names being listed in the bibliography or other references).

3.6 Be in either English or Afrikaans.

3.7 The use of abbreviations in the manuscript should be avoided as far as possible.

3.8 It is strongly recommended that authors have their manuscripts reviewed for language proficiency before submitting them, as excellent submissions sometimes have to be drastically amended or even rejected because of linguistic ineptitude. The editor reserves the right to make *minor* editorial adjustments without consulting the author (also refer to the condition of final linguistic editing as set out under the heading “The reviewing and publishing process”).

3.9 The manuscript has to be submitted in the following electronic formats: one MS Word file *as well as* one pdf file.

3.10 The file name must be designed in the following format: author’s surname – short title of the article – date of submission (yyyy-mm-dd). For example: Smith – *Accountability in the public sector – 2013-11-01*. Where a second author is involved, give second author’s surname after first separated by a “-“. *For example: Smith – Jones – Accountability in the public sector – 2013-11-01.* Where more than two authors are involved use “et al” after first author. For example: *Smith et al – Accountability in the public sector – 2014-04-14.*

The following *reference technique* must be followed:

3.11 References should be inserted into the text by indicating in brackets the name of the author(s) and the year of publication of the quotation for example "...Jones (2013) states that...", or "...that the going concern concept is not applicable for these purposes" (Jones 2013).

3.12 If reference is being made to a specific page, a colon follows the year of publication (no spaces), followed by the page number (again, no spaces), for example: "...Jones (2013:18) states that...", or "...that the going concern concept is not applicable for these purposes (Jones 2013:18).

3.13 If the specific author has more than one publication in any one year, the articles are distinguished by inserting the letters a, b etc. after the year of publication, for example: "...Jones (2013a:18) states that...".

3.14 Footnotes may not be used for reference purposes.

The *Bibliography* has to be prepared according to the following standards:

3.15 Publications referred to in the text are listed alphabetically by surname of the first author.

3.16 References to the same author appear in the sequence of publication, and if an author has more than one publication in any one year, the articles are distinguished by adding the letters a, b etc. after the year of publication (see standards for the *reference technique* above).

3.17 In the case of articles in journals, details of each article should appear in the bibliography in the following sequence: surname, initials (or names, if used in the original publication), year of publication, title of article, name of journal (in italics), date or number of journal. In the case of books, details of each book should appear in the bibliography in the following sequence: surname and initials (or names, if used in the original publication), date of publication, title of book (in italics), name of publishers and place of publication.

3.18 The bibliography is not subdivided into sections for books, journals, papers, etc.

Examples:

Jones, P. 2017. The Going Concern Concept. *Auditing SA.* January:page number(s).

Jones, P. 2013. *Auditing.* 2nd edition. Pretoria: Unipret Publishers.

Jones, P., James, C. & Johnson, B.C. 2013. The Going Concern Concept. *Auditing SA.* January 2013.

Gay, G., Schelluch, P. & Reid, I. 2011. Users' perceptions of the auditing responsibilities for the prevention, detection and reporting of fraud, other illegal acts and error. *Australian Accounting Review*, 7(1):51-61.

Lawrence, G.M. & Wells, J.T.Y. 2013, *Basic Legal Concept.* [Online].
http://www.aicpa.org/pubs/jofa/oct2004/lawrence.htm
(Accessed: 12 December 2013).

Southern African Institute of Government Auditors (SAIGA). 2014. *Common Body of Knowledge and Skills for Registered Government Auditors, CBK 001*. January, SAIGA. Pretoria: Menlo Park.

The following *layout standards* have to be adhered to:

3.19 Each drawing or table must be provided with a concise, unique heading.

3.20 Footnotes should be avoided as far as possible. Footnotes are only permissible when it is necessary to clarify a specific point, and it is undesirable to include the explanation in the text, because the logical flow of the argument may be disrupted. Such footnotes appear at the bottom of the page to which they refer. On each page footnotes start with number 1.

3.21 Endnotes are permissible.

3.22 The use of bold typeface in the text should be avoided as far as possible. Accentuation should be done by using italic typeface. Foreign words (e.g. pro rata, status quo, etc.) should be in italic typeface.

3.23 Direct quotations from other publications should be avoided. Such quotations are only permissible in exceptional circumstances when the specific quotation is so succinct and vivid that the text may be materially enhanced by the quotation.

3.24 Headings are numbered 1, 2 etc., and sub-headings 1.1, 1.2 etc. More than three characters (points excepted) in a sub-heading (points excepted) are not permissible. All headings and sub-headings appear adjacent to the left margin in bold (not capital letters). If bold typeface is not available, headings and sub-headings are underlined.

3.25 Acknowledgements of financial and other assistance should be formulated in an end note.

3.26 Acknowledgements of a highly personal nature are not permissible.

Other *administrative rules* that are applicable:

3.27 The submission must be e-mailed to *secretary@saiga.co.za* and addressed to: The Editor, SA Journal of Accountability and Auditing Research. No other e-mail address may be used.

3.28 Incomplete or off-standard manuscripts are not returned. Authors are notified by the Secretariat and a new set of manuscripts and/or other elements of the submission must be lodged with the Institute.

3.29 It is a condition of acceptance that, irrespective of any linguistic work already done on the article, each article will be sent to the Institute's linguistic editors before final publication (for details regarding linguistic fees see above).

3.30 SAJAAR does not accept manuscripts that are submitted to other journals.

3.31 No new manuscripts may be submitted to review and publishing if any fees, relating to previously published articles by an author, are still outstanding.

3.32 Authors(s) have to undertake not to submit the manuscript to another journal, until such time as SAJAAR's Editor, has informed the author(s) that the article cannot be published and has allowed the author(s) to withdraw the article.

3.33 If the manuscript has previously been submitted to another journal and withdrawn or rejected by that journal, the correspondence in this regard will have to be submitted.

3.34 Manuscripts that have been read at conferences or disclosed at public forums or events, whatever nature, are not appreciated and will only be considered in exceptional circumstances.

3.35 Copyright of published articles is transferred to the *Southern African Journal of Accountability and Auditing Research*.

3.36 Each author will receive five complimentary copies of the *Southern African Journal of Accountability and Auditing Research* (authors can obtain more copies on request at a nominal price).

3.37 SAIGA has instituted an annual *Research Award*. Articles published in the scientific journal *SAJAAR* are automatically eligible for the *SAIGA Research Award*. A panel of international experts, comprising of academics and senior government auditors make a recommendation to the Council of the Institute which makes the final decision. The *SAIGA Research Award* aims to encourage and support independent research and discourse. The *SAIGA Research Award* is not an annual event, but its occurrence will be determined by the Executive Committee of SAIGA.

4 The signed declaration

The author(s) have to sign a declaration stating the following (please note that the specimen letter available on our website [in pdf format] has to be used to comply with this requirement):

4.1 That the manuscript is submitted to SAIGA with the full intention of having it published in the Southern African Journal of Accountability and Auditing Research.

4.2 That they understand the reviewing and publishing process followed by SAIGA and that they agree to submit the manuscript under these conditions and rules.

4.3 That the article constitutes their original work; that other authors' work has been quoted by applying normal practices in this regard; that they indemnify the Institute from any copy right infringement which may result from the publishing of the manuscript.

4.4 That the manuscript has not been submitted to another journal or if it has been submitted to another journal and withdrawn or rejected, they must provide SAIGA with the correspondence in this regard.

4.5 That the manuscript has not been read at any conference or disclosed at public forums or events, whatever nature or published in any form whatsoever.

4.6 That they understand that the manuscript may not be withdrawn or submitted to another journal whilst the reviewing process is underway, unless the Editor specifically allows the author(s) to withdraw the article.

4.7 That they agree to the conditions of payment of the linguistic and page fees.

The signed declaration must be submitted as a pdf file and the file name must be constructed as follows: Surname of author – Signed Declaration – date of submission (yyyy-mm-dd).
For example: *Smith – Signed Declaration – 2014-04-14*.

5 Electronic submissions only

Submissions can only be done electronically. The submission must be e-mailed to *secretary@saiga.co.za* and addressed to: The Editor, SA Journal of Accountability and Auditing Research.
No other e-mail address may be used.
File names must be constructed in the required file format.
Every submission must contain FIVE files: covering letter (pdf); the information sheet (pdf); the manuscript (MS Word and pdf) and the signed declaration (pdf).

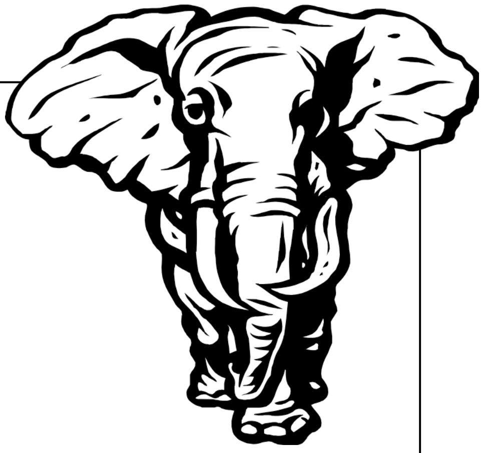
Auditing SA

A semi-scientific journal, published by the Southern African Institute of Government Auditors to advancing discourse in Auditing and Accountability.

Auditing SA offers academic scholars the opportunity to publish their results for a wider audience – communicating their findings in less formal style.

For more information
Visit the SAIGA website
www.saiga.co.za

ADVANCING ACCOUNTABILITY



If it comes to
STRENGTH
he is in a class of his own

At the Southern African Institute of Government Auditors (SAIGA) we view Government Auditing from a different perspective.

Our members perform this function for the benefit of all South Africans. Because Government Auditing advances accountability and good governance.

Our members' vision and determination helped develop Government Auditing to its current levels.

SAIGA salutes all Registered Government Auditors (RGAs)

You are in a class of your own.

The South African Qualifications Authority (SAQA) has recognised The Southern African Institute of Government Auditors as a professional body for the purpose of the National Qualifications Framework Act, Act 67 of 2008.

ADVANCING ACCOUNTABILITY

The professional designation "Registered Government Auditor" (RGA) is also registered on the National Qualifications Framework (NQF) for the purposes of the NQF Act of 2008.

The Southern African Journal of Accountability and Auditing Research

EVOLVING RESEARCH

SAIGA

ADVANCING AUDITING AND ACCOUNTABILITY

PO Box 36303 Menlo Park 0102 South Africa
Tel: 012-362-1221 Fax: 012-362-1418

Evolving Research

SAIGA

ADVANCING AUDITING AND ACCOUNTABILITY