The Southern African Journal of Accountability and Auditing Research

Vol 18: 2016 ISSN 1028-9011

Contents of this issue

Published by the Southern African Institute of Government Auditors

SAIGA

ADVANCING AUDITING AND ACCOUNTABILITY

The Southern African Journal of Accountability and Auditing Research

Vol 18: 2016 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: admin@saiga.co.za

Website: www.saiga.co.za
NPO No: 045-133-NPO

V&R Printing Works, Pta. Tel: 012 333-2462

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

EDITORIAL COMMITTEE

REVIEWERS

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

Evaluate the effectivity of a newly developed audit simulation to improve the perceived broad competence of audit students

R de Villiers

School for Accounting Sciences
North West University

ABSTRACT

Audit education is in need of change with regard to the teaching methodologies utilized at universities including other institutions of higher learning, both locally and globally. This need is evident by the robust volume of research highlighting the current criticisms against audit education in the form of the out-dated teaching methods employed by audit lecturers. These methods include a passive learning approach. Moreover, the fact that the teaching is concept-oriented, often results in students' having difficulty in understanding audit concepts through the lack of a clearly developed and adequate frame of reference. This study forms part of a bigger project, in that an audit simulation was developed to meet these needs. The objective was to evaluate whether the newly developed audit simulation would assist to enhance audit students' perceived broad competence, and to draw conclusions as well as suggest recommendations on the use thereof in the audit classroom in light of the current criticisms. The research approach included the classic quasi-experimental (pre-test/post-test) design to reach the objective of the study and a group-administered questionnaire to collect data from the respondents. The results of the pre-test/post-test evaluation revealed that change is needed of the manner in which auditing is taught at universities and other institutions of higher learning. Furthermore, it was found that by adopting teaching methodologies such as this newly developed audit simulation, positive change can be brought to the audit education environment. Certain areas for further research and development were also identified together with recommendations on the use of simulation in the audit classroom.

Key words

Audit education; audit simulation; audit student; broad competence

1 INTRODUCTION

There is an on-going debate about what the audit student should know and be able to do after graduation and upon entry into audit practice. Ulrich, Michenzi and Blouch (2011:935) stated that literature on accounting revealed that audit practitioners are dissatisfied with the education that audit students are receiving at universities or other institutions of higher learning. The authors further stated that:

> "Practitioners expect new accounting graduates to have a reasonable degree of practical skill in auditing while educators believe that it is the practitioners' responsibility to train their entry-level auditors how to audit" (Ulrich, Michenzi & Blouch 2011:935).

Internationally, several researchers in the field of audit education have stressed the need for change in the approach followed to teach auditing at universities and other higher education institutions (Barac 2012:51; De Lange, Jackling & Gut 2006:365-370; Saunders & Machell 2000:290; Tan, Fowler & Hawkes 2004:51-53). This call for change transpired as a result of the accounting profession's emphasis that it is not merely the technical knowledge of auditing that must be understood by students, but they should also be able to apply this knowledge and have a number of generic and pervasive skills to enhance the audit students' ability to be hired and to apply themselves in public practice (Saunders & Machell 2000:290-298; Tan, Fowler & Hawkes 2004: 51-53).

In South Africa, the South African Institute of Chartered Accountants (SAICA) in 2010 established a competency framework (version 2; issued on 22 October 2010) which outlined the competencies required of Chartered Accountants (CAs) in South Africa upon entry into the auditing profession (SAICA 2010:6). This competency framework was developed based on extensive research into international trends and local consultation with practitioners which included a substantial amount of input from the academic world (Olivier 2014). Barac (2012:51) explained that this competency framework was established by SAICA to specify or clarify the expected competencies for entry-level CA's which differs from the past practice where SAICA prescribed syllabi to be followed by accredited universities or other higher education institutions. SAICA stated that

this introduction of a competency framework, as part of the curricula followed at SAICA-accredited higher education institutions, will ensure that individuals entering the profession have the necessary knowledge and practical skills to perform the required tasks of a CA in today's business environment (SAICA 2010:3).

This competency framework, therefore, requires a CA to have mastered a broad range of competencies when entering the profession. This ensures that a CA is seen as a leader in the professional accounting environment (SAICA 2010:4) and is perceived as competent in: i) strategy, risk management and governance; ii) financial management; iii) auditing and assurance; iv) accounting and external reporting; v) taxation; vi) management decision making and control; and, finally vii) generic and pervasive skills, such as ethics and professionalism, personal attributes and professional skills (SAICA 2010:4). The implementation of this competency framework can, therefore, be perceived as an attempt by SAICA to answer this global call for change in audit and accounting education in general due to the inclusion of competency requirements specifically for auditing and assurance as well as generic and pervasive skills. This competency framework, if implemented correctly at tertiary level, will assist in filling the gap between what practitioners want audit educators to teach, and what audit educators think they should be teaching.

In filling this gap, audit lecturers have to incorporate not only the technical competencies of the audit subject, but also a number of generic and pervasive skills in order to develop audit students who are more competent when entering professional practice after graduation. In doing so, an attempt can be made by audit lecturers to answer the call from practice to deliver students to the market place who have not only mastered the technical content of the audit subject, but are also able to apply these principles in professional practice, in addition to demonstrating a variety of generic and pervasive skills. The latter will aid in bringing about change in the approach that is followed in audit education today. Although this might seem to be a simple solution to the current dilemma faced by audit education, the question that remains to be answered encompasses what method(s) audit lecturers should apply in the audit classroom to assist them in incorporating these competency requirements into their curricula as well as ensure that their students are given the opportunities to develop these competencies.

In an attempt to answer this question, the remainder of the study is structured as follows: the past and current approaches followed in audit education are discussed followed by an overview of the extant volume of literature on the use of audit simulations as a teaching tool in the audit classroom. This is followed by the problem statement of the study and a description of its research objectives and intended value. How the simulation was designed is discussed next. Finally, the research design and empirical findings are discussed, conclusions are drawn on the basis of the results, the limitations of the study are identified and certain areas for further research and development are highlighted.

2 PAST AND CURRENT APPROACH TO AUDIT EDUCATION

Auditing courses are generally concept-oriented and students often grapple to relate to these ideas due to the lack of a clearly developed and adequate frame of reference to analyse and understand these auditing concepts (Arens, May & Dominiak 1970:573). Siegel, Omer and Agrawal (1997:218) support the statement made by Arens *et al* (1970:573) that audit students at higher education institutions lack experience with transactions and activities which constitute the subject matter of auditing. They further assert that this lack of 'feel' introduces a roadblock for students in their journey to comprehend basic auditing concepts and ideas and consequently results in a lack of academic performance in this subject field that forms part of their curricula (Siegel, Omer & Agrawal 1997:218).

This deficient understanding of auditing models by students was recently evaluated by various researchers in the field of accounting education, e.g. Hosal-Akman and Simga-Mugan (2010) as well as Steenkamp and Von Wielligh (2011). This has resulted in various criticisms against the methods applied by audit educators to assist students in their grasp of auditing at under- and postgraduate levels.

The first of these criticisms points to the teaching approach followed by audit lecturers (Hosal-Akman & Simga-Mugan 2010:251; Steenkamp & Von Wielligh 2011:9). Courses in accounting degrees frequently apply out-dated methods and follow a passive learning approach which require students to sit down in a classroom and merely listen to the lecturer for hours on end, resulting in a situation where there is no active student participation in the learning process (Hosal-Akman & Simga-Mugan 2010:251; Siegel *et al* 1997:217; Steenkamp & Rudman 2007:23). This passive technique of conveying auditing theory to the untried young auditor in the making has in numerous instances resulted in poor results when their audit knowledge is examined (Siegel *et al* 1997:218).

A further critique of audit education relates to the method of examination, where students are assessed on their competence by means of a written examination (Botha 2001:42). Botha (2001:42) expressed concern about this method by stating that:

> "… demonstrating that one can successfully negotiate a written examination, which primarily tests knowledge, is not the same as possessing the skills and attitudes required for professional practice. It is wrong to claim that a final written qualification examination, which in essence tests a student's knowledge, is an assessment of a practitioner's competence".

Although these two criticisms have been highlighted by several other studies, such as that of Barac (2012), the predominant issue identified throughout in the body of audit education research relates to the absence of practical experience in audit training (see Barkman 1998:517; Tonge & Willett 2012: 171; Worrell 2010:538). These researchers stressed the importance of introducing students to actual

situations, i.e. by developing case studies or simulations that will enable them to be active participants in the learning process and therefore be exposed to some form of practical experience (Barkman 1998:517; Tonge & Willett 2012:171; Worrell 2010:538).

Turning attention to the use of simulations as a learning tool in audit education, an abundance of studies have been performed in this regard which have recognised the advantages this method can bring to enable students' understanding of auditing as well as in assisting them to become competent in audit specialism (Bagley & Harp 2012; Gelinas, Levy & Thibodeau 2001; Miller & Savage 2009). These cited studies, though not an exhaustive list, have developed audit simulations applied at specific higher education institutions around the world, adding significant value to audit education in general, thus warranting attention in the literature review to follow.

3 PREVIOUS USE OF AUDIT SIMULATIONS: A LITERATURE REVIEW

A variety of audit simulations has been developed over the decades to assist auditing students at institutions of higher learning to master the audit of financial statements. Arens, *et al* (1970) designed a simulation project that provided a frame of reference to discuss factors that affect auditors' decisions in developing audit programmes together with determining the extent to which a financial statement account should be audited. Whilst conducting this project, the students had limited exposure in physically performing the audit procedures they developed for inclusion into the audit programme (Arens *et al* 1970).

A simulation model for applying audit-sampling techniques was reported by Walgenbach and Frank (1971) from the University of Wisconsin in the early 1970s. In this paper they contributed to the existing computer-simulated audit performed by students of this university including those who were enrolled for auditing courses (Walgenbach & Frank 1971:583). Since then no other literature was identified that contains the audit-sampling process as part of a simulation. A number of years later, Weber (1978) established a model to support auditor decision-making in overall system reliability. This paper examined certain facets of the external auditor's judgement process in evaluating the overall reliability of internal control for a company's inventory system (Weber 1978).

Krogstad, Smith, and Clay (1986) examined the impact of a simulation of audit practice on students' attitudes and perceptions about a variety of factors pertaining to auditing. These factors included: i) the importance of human relations skills; ii) professionalism; iii) prerequisite knowledge of accounting and auditing standards; and iv) career opportunities in auditing (Krogstad *et al* 1986:309). In this study, simulations proved to be an effective tool in assisting students in experiencing many aspects of the audit process.

Siegel *et al* (1997:217-230) made use of an audit video simulation. This paper reported the results of a controlled experiment conducted to apply experiential learning theory to teaching auditing (Siegel *et al* 1997:217). In this experiment, a series of videotapes were provided to students to equip them with a view of what essentially occurs in an audit. These videotapes formed part of an active learning approach. The videos were applied as visual aids to assist students in their understanding of what actually happens during the audit process (Gawe, Jacobs & Vakalisa 2012:215-246; Lasley & Ornstein 2004:297-320).

In 2001, Gelinas, Levy and Thibodeau (2001) constructed a simulation wherein auditing students were introduced to computer-assisted audit techniques in the audit process. In this simulated audit, participants became accustomed to the use of audit software in performing audit procedures as well as in identifying audit risks and the setting of an audit approach, resulting in improved audit technology and critical thinking skills (Gelinas *et al* 2001:610).

Borthick and Curtis (2004:Online) reported on the use of an audit simulation for due diligence on a fashion inventory through data querying. Whilst carrying out this exercise, the students designed audit procedures to test the audit assertions such as inventory completeness and existence. They reported on the findings and unresolved issues together with the lessons learned from this study (Borthick & Curtis 2004:Online). The learning objectives of this simulation comprised the development of essential skills such as verification of internal consistency of accounting records and the detection of issues that would require further investigation by the auditor (Borthick & Curtis 2004:Online). This experience offered the students the opportunity to bridge the gap between theory and practice.

Steenkamp and Rudman (2007) studied the usefulness of an audit simulation by obtaining student perceptions at a South African university. In this study, students had to prepare auditing inventory working papers and a database large enough for students to make use of Information Technology (IT) to assist them in the process (Steenkamp & Rudman 2007:23). This simulation also indicated that significant value is added to student learning by means of a simulation.

In more recent years, Miller and Savage (2009) developed an audit simulation to help students in applying audit procedures that pertain to revenue recognition. In particular, the students gained a better understanding of the importance of management's occurrence, accuracy and cut-off assertions of revenue as well as how the connection is made between an audit procedure and an audit assertion (Miller & Savage 2009:93). This simulation further embarked on providing students the opportunity to physically perform audit procedures of revenue as well as document their findings on working papers (Miller & Savage 2009:93).

Worrell (2010) developed a simulation focusing purely on the procurement section of an audit. In this audit simulation, audit procedures were conducted as part of a business process unit, to assist students to understand and perform procurement audit work by

providing them with a realistic setting to conduct audit procedures expected from interns and entry-level auditors (Worrell 2010:527). Worrell also introduced the use of blended learning by adding interviews with clients in MP3 file format to assist students to obtain certain required information to perform the audit procedures. Worrell concluded that audit simulations effectively simulate a real-world audit and are immensely treasured by students, not only in developing the audit skills, but also in helping to trigger interest in the audit profession (Worrell 2010: 539).

Bagley and Harp (2012) reported on the use of audit simulation in auditing the property, plant and equipment, and depreciation section of the financial statements of a simulated client. The students were provided with electronic working papers that included an audit programme, client-prepared documents as well as prior year working papers (Bagley & Harp 2012:1131). This simulation had several objectives: the first being to familiarise students with electronic working papers and allowing them to be exposed to Microsoft Excel in an audit environment; secondly, to provide students with the opportunity to audit PPE and its related depreciation expense by applying substantive analytical and detail testing; thirdly, to test the evaluation of internal control and its implications on the audit approach; and lastly, to develop soft skills such as writing and client interview skills (Bagley & Harp 2012:1131).

Tonge and Willett (2012) introduced an audit simulation that took the form of a financial systems audit or review for a large local charity. They anticipated that performing a genuine audit activity for a 'real client' would bring exclusive benefits in terms of inspiration to obtain and apply technical expertise (Tonge & Willett 2012:172). In addition, they introduced the necessity to work under pressure in small teams to inspire team-work growth and communication skills. This project covered audit sections such as risk management, revenue and procurement (Tonge & Willett 2012:175).

From the aforementioned studies, it is clear that certain international researchers have been attempting to ameliorate the criticisms against audit education for several decades by incorporating audit simulations as part of their teaching methodology. However, Tonge and Willet (2012:171) stressed that students are still finding auditing perplexing and difficult despite the various attempts by researchers to address the issues in audit education. Furthermore, it was also noted from the literature that although numerous studies on the use of simulations in *certain* steps of the audit process have been conducted, none have been performed where audit simulations have been employed for the *entire* audit process. It can, therefore, be concluded that there is a clear need for further comprehensive research on an effective approach in teaching auditing at universities or other institutions of higher education. The latter is imperative if an attempt is to be made to bring change to the methodology applied in audit classrooms around the globe. Against this background, the research objective and the value that this study intends to add are discussed next.

4 PROBLEM STATEMENT

The approach followed to date, in preparing audit students at higher education level for the actual auditing environment that they will form part of, still requires change. This change may assist in answering the auditing profession's call for students to be more actively involved in the process of developing the necessary skills and knowledge to be able to conduct an audit in terms of the International Standards on Auditing (ISAs). To date no comprehensive study has been conducted which incorporates the entire audit process and broad competency requirements of the SAICA competency framework addressing the latter shortcoming.

5 RESEARCH OBJECTIVES AND VALUE

With reference to the problem stated earlier, it is essential that more interventions are needed with regard to the audit education approach followed at universities and other higher education institutions. This study forms part of a bigger project, where an instrument, i.e. an audit simulation project for implementation at universities and other higher education institutions in South Africa and globally, was developed to grant students the opportunity to develop the various competencies related to auditing and assurance, as well as generic and pervasive skills, as stipulated in the SAICA competency framework.

In this study, the objective was to evaluate whether this newly developed audit simulation would assist in enhancing the audit students' perceived broad competence (i.e. auditing and assurance as well as generic and pervasive skills competencies) and to draw conclusions as well as provide recommendations on the use thereof in an attempt to bring change to the current approach followed in audit classrooms.

No local or international studies of this calibre, which specifically incorporate the SAICA competency requirements as well as the entire audit process have been identified throughout the literature review. This finding, therefore, makes a study of this nature contemporary, warranted and in desperate need. This study further contributes to audit education in general, by reporting on the use of a renewed and an up to date audit simulation incorporating the latest auditing standards and other legislation to be implemented at universities, training offices as well as other higher education institutions globally. This newly developed audit simulation will, in its own right, also contribute considerably to audit education in general and could assist audit educators around the world in preparing audit students for the hard reality of practice.

The aforementioned contributions are also internationally invaluable as they pertain to the broader accounting and auditing profession outside of a South African context due to the fact that the criticisms against the current approach followed in audit education, noted throughout the internationally cited literature in this study, revealed that this is currently a globally recognised phenomenon. Furthermore, the ISAs is also applied internationally.

The findings of the study and recommendations should be valuable to audit educators globally.

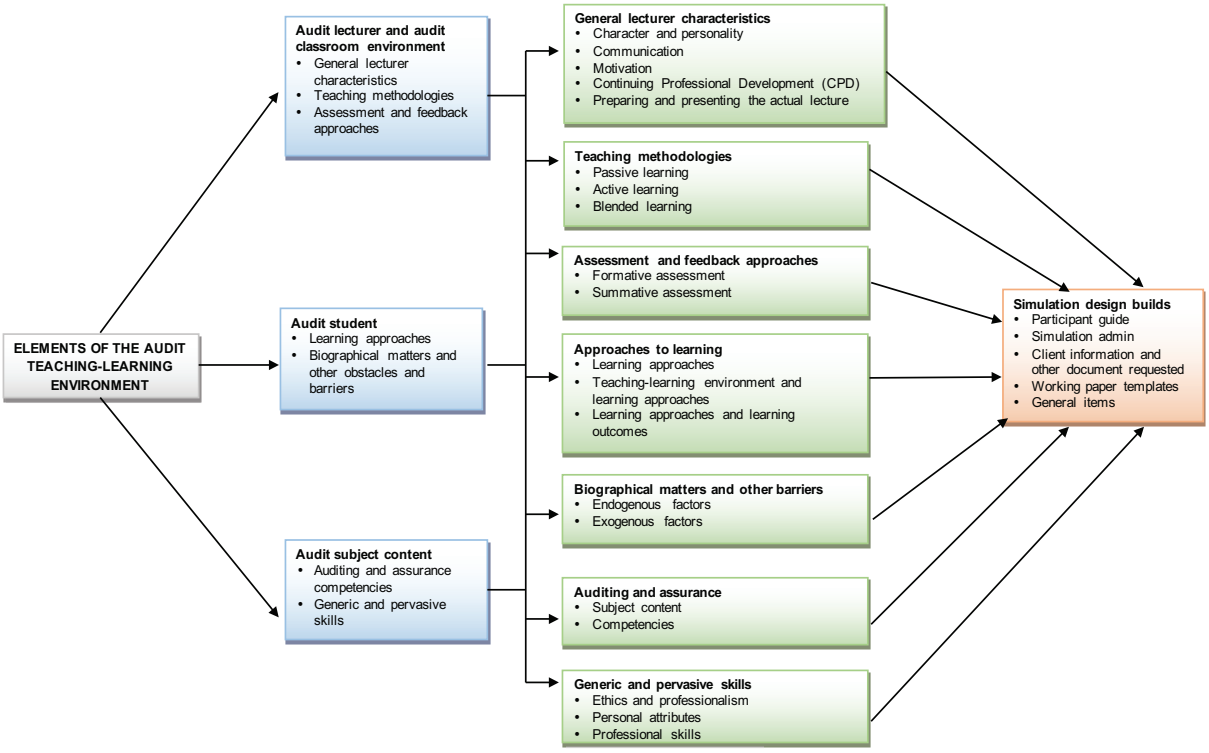
6 DESIGNING THE AUDIT SIMULATION AS EDUCATIONAL TOOL

As a starting point to developing the audit simulation project, the author conducted a literature review to identify a framework for simulation design. This was done in order to:

- Specify all the relevant variables that need consideration;
- Ensure that the research in developing simulations in general is conducted systematically; and
- Mitigate issues that would result in ineffective development and practice (Jeffries 2005:97).

According to Fouché (2006:131), simulations and games that are used for educational purposes need to be designed effectively as well as incorporate all the variables in the overall teaching-learning environment. These include the audit lecturer, the audit classroom environment, the audit student and the audit subject content (Fouché 2006:131). After performing an extensive literature review, the author could not identify a framework for simulation design that incorporates all the variables in the overall audit teaching-learning environment. Therefore, an attempt was made to develop a framework that could be applied in designing the new audit simulation which includes the specific motivations with regard to the variables of the audit teaching-learning environment, as noted from the extensive literature review. Figure 1 demonstrates the framework for simulation design developed by the author which includes all the variables and their specific considerations for inclusion in the simulation design as acquired from the literature.

Figure 1: Framework for simulation design



Source: Author

The next step was to develop the five primary builds in the simulation design which comprised the physical substance of the newly developed audit simulation. These included the participant guide; simulation admin; client information and other requested documents; working paper templates; and general. These builds were used to develop the audit simulation entitled 'Finance Master (Pty) Ltd, an audit simulation performed by R&R Auditors Inc.' In this audit simulation, the client that was audited was referred to as Finance Master (Pty) Ltd, whereas the students performed the role of R&R Auditors Inc. The builds and their relevance to the audit simulation are clarified in the discussion in the following paragraphs.

The participant guide contains all the subject content requirements, client background and information, instructions and guidance needed for the tasks to be performed by the students in completing the audit simulation. In order to successfully perform the audit simulation, students need to read this guide from start to finish and follow instructions in each step of the audit process.

The simulation admin build consists of a variety of documents to be used throughout the audit simulation, such as a kick-off meeting agenda and a team member's assessment document. During the different sections of the audit simulation, students are

referred to the relevant documents when needed.

Client information and other documents requested comprises a variety of client documents (audit evidence) needed to perform the tasks required by each stage of the audit simulation. These include invoices, bank statements and loan contracts. Working paper templates required to perform different tasks during the simulation exercise are provided to the audit teams (the participants) in either Microsoft Word or Microsoft Excel format. These working papers need to be completed by the participants in the audit simulation. The general build represents other tangible and intangible aspects of the audit simulation. Tangible aspects include the use of flyers and banners as visual aids, whereas intangible aspects are, for example, the application of effective lecturer characteristics such as being friendly and approachable during the audit simulation. It further represents intangible generic and pervasive skills such as teamwork ability.

7 RESEARCH DESIGN AND METHOD

7.1 Overall research design, population and sample selection

A quantitative study, in the positivistic paradigm, that applied the classic quasi-experimental (pre-test/post-test) design was followed to evaluate the audit simulation in combination with a group-administered questionnaire. The selection of the quasi-experimental design was based on the fact that it will contribute to the reliability and validity of the experimental design (Fouché 2006:149). Experimental research is defined by Creswell (2005:52) as research that determines whether an intervention influences an outcome for one group as opposed to another. Experimental research encompasses having an experimental group that receives the intervention and a control group that does not receive the intervention.

The target population of the study consisted of third-year audit students in the CA programme at two South African universities accredited with SAICA. The experimental group consisted of the third-year audit students at University X and the control group consisted of the third-year audit students at University Y. University Y was selected as the control group for the experiment after considering the mediating variables such as age, race, gender and level of education, i.e. the biographical background of the respondents to ensure that the results of the experiment are reliable, and that minimal differences, if any, are present in the variables affecting the experiment's respondents.

In so doing, the author attempted to ensure that the mediating variables did not affect the reliability and validity of the data obtained as this is an important consideration in quantitative research (Chung, Shin, Oh, & Lee 2013:455; McKerchar 2008:11). The effect of these mediating variables, if any, that may result in differences between the experimental and control group, and how it was accounted for in further ensuring the validity and reliability of the data, are discussed later in the analysis of the empirical findings. Moreover, the author is confident that University Y is an acceptable control group after considering the following observations and findings:

- The curriculum content of the audit subject at both universities is governed by SAICA;
- The audit curriculum programme proved to be structured in the same manner for both universities, resulting in these students' having covered the same audit subject content requirements up until the time the study was performed;
- Discussions held with the lecturers responsible for the audit subject for the third-year audit students at both universities confirmed that the past teaching methodologies and assessment and feedback approaches applied by these lecturers were the same in the majority of cases; and
- The textbooks and auditing standards used for studying by the students of University Y were found to be the same as those used at University X.

Furthermore, no other control group (SAICA-accredited university) was identified that related similarly to the sample size and demographical variables such as age, race and gender and cultural background, as did University Y. In addition, the author is confident that the sample population used in the experiment provided reliable results as the group-administered questionnaires were distributed to sample populations affected by the same phenomena under investigation in this study.

In addition, the sampling rate limitations were addressed, because the entire population affected by the phenomenon under investigation was considered at both University X and University Y. All the third-year audit students in the CA programmes at both universities, attending class at the time the pre-test and post-test questionnaires were administered, were invited to complete the questionnaires. In doing so, the sampling bias was restricted and good response rates were obtained for the pre-test that represented 73% (531), and the post-test that represented 68% (495) of the target population, which consisted of a total of 725 third-year audit students for both universities. This mitigates a variety of the design threats inherent in the use of questionnaires as an instrument of data collection. It should be noted that participation by the students was voluntary and that the confidentiality of the information provided by the students was emphasised and assured to the students. Ethics clearance was also obtained from both universities before the questionnaires were distributed to the respondents.

Table 1 below provides information with regard to the profile of the sample population used in this study. It is deemed important to consider these factors in the analysis of the data to ensure the research findings are comparable to those of other research conducted in this field of study. Furthermore, the results of the biographical analysis presented confirms the author's argument that the sample population is well represented at both universities, that is, to any mediating variables as discussed earlier that may affect the comparability of the results obtained in this study. It should also be noted that these biographical results include all the students who completed the pre-test and post-test questionnaires at the time the questionnaires were

administered. In determining the effect of the simulation on the audit students' perceived broad competence, the results only include students who completed both the pre-test and post-test questionnaires. Hence, only students who completed both the pre-test and post-test questionnaires are included in the latter analysis.

Table 1: Profile of the sample population participating in the experiment

Respondent groups	**Pre-test**		**Post-test**	
	N*	**%**	***N****	**%**
University X (Pre-test, Simulation, Post-test)	311	58.6	305	61.4
University Y (Pre-test, Post-test)	220	41.4	191	38.6
Gender	**Pre-test**		**Post-test**	
	N*	**%**	***N****	**%**
Female	318	59.9	238	48.1
Male	213	40.1	257	51.9
Races	**Pre-test**		**Post-test**	
	N*	**%**	***N****	**%**
Black	206	38.8	180	36.4
White	291	54.8	281	56.8
Coloured	17	3.2	19	3.8
Indian	11	2.1	10	2.0
Asian	0	0	2	0.4
Other	6	1.1	3	0.6
Mother tongue	**Pre-test**		**Post-test**	
	N*	**%**	***N****	**%**
English	29	5.5	32	6.5
Afrikaans	288	54.2	284	57.3
An African language	194	36.5	152	30.7
Other	20	3.8	27	5.5
Enrolment status	**Pre-test**		**Post-test**	
	N*	**%**	***N****	**%**
Full-time	507	95.5	471	95.2
Part-time	24	4.5	24	4.8
Student's level of practical experience in audit practice	**Pre-test**		**Post-test**	
	N*	**%**	***N****	**%**
0 months	367	69.1	344	69.5
1–6 months	107	20.2	108	21.8
12 months	16	3.0	17	3.4
More than 12 months	41	7.7	26	5.3

**Frequency*

Conducting the experiment

The third-year audit students in the CA programme at both University X (being the experimental group in the experimental design) and University Y (being the control group in the experimental design) were asked to complete the pre-test questionnaire in the same week of the academic year at separate campuses of the respective universities. The experimental group (University X) was then asked to complete the audit simulation over a period of 10 weeks and to submit the completed simulation at the end of the 10th week, whereas the students of University Y continued with their normal lectures in auditing without completing the audit simulation, i.e. did not participate in the simulation (intervention). The post-test questionnaire was then completed by the students at University X and University Y who participated in the experiment within one week after completion of the simulation by the third-year audit students at University X. It was confirmed, through discussions with the lecturers responsible for the third-year audit subject, that the students at University X and University Y did not participate in any other audit simulations or other active learning methodologies before or during the experimental period and up until completion of the post-test questionnaire. Table 2 illustrates the process followed in conducting the experiment.

Table 2: Quasi-experimental design

Type of group	**Group no.**	**Pre-test questionnaire**	**Newly developed simulation**	**Post-test questionnaire**
Experimental	University X	√	√	√
Control	University Y	√		√

7.2 Developing the questionnaire

As noted from the research design discussed earlier, a group-administered questionnaire was adopted to gather the data for this study. Questionnaires have possible design limitations or weaknesses, therefore, it was imperative to ensure that a properly designed questionnaire and its effect on the validity and reliability of the data obtained from respondents are considered. Blair, Blair, and Czaja (2014:177) argued that researchers must approach the task of constructing a questionnaire not as an isolated effort, but as one informed by the research objectives. In doing so, the structure, purpose, validity and reliability of the

questionnaire design which requires consideration is discussed next.

The purpose of the questionnaire was determined by making reference to the objective to be met, that is, to evaluate whether a newly developed audit simulation would assist in enhancing audit students' perceived broad competence. In order to achieve this objective, the pre-test and post-test questionnaires were divided into seven primary sections with the questions being framed based on the competency requirements for auditing and assurance informed by the subject content as well as generic and pervasive skills. The latter was obtained from the SAICA competency framework discussed earlier (SAICA 2010). These questions consisted of six demographical questions (Questions 1 to 6) and 171 (Question 7 to 177) five-point Likert-type closed-ended questions probing the views of students on whether the current teaching methodology applied in the audit classroom of their respective universities effectively assists and enables them to be deemed competent in auditing and assurance as well as in the generic and pervasive skills. The scores on the five-point Likert-type scale that the students applied to these questions ranged from: 1 (Not at all); 2 (Very little); 3 (Somewhat); 4 (Quite a bit); to, 5 (To a great extent).

The last section (only included in the post-test questionnaire) included questions on the audit students' attitude towards the audit simulation (Question 178 to 186) as Noyes and Garland (2005:234) noted that the students' attitude towards an object influences their behaviour and may impede the learning that should take place by performing the simulation. The author, therefore, deemed it appropriate to measure the audit students' attitude towards completing the audit simulation based on the attitude measure developed by Kay in 1989, which was revised in 1993, and applied by Noyes and Garland (2005:234). Fouché (2006:154) and Van der Merwe (2013:152) also applied this attitude measure in their research, and reported that this measure revealed valuable insight on students' attitudes towards an instrument applied as an educational tool.

In an attempt to mitigate threats to validity and reliability that could be ascribed to its design given that the questionnaire was newly constructed and no suitable existing instrument was available that specifically measures audit students' perceived competence on the SAICA competencies, the author implemented several techniques or procedures in an effort to ensure reliable and valid results. The validity, reliability and completeness of the questions were ensured through accurately compiling questions based on the competencies informed by the related subject content requirements. The questions were also examined by a number of experienced research and audit academic professionals at University X as well as a qualified statistician at the Statistical Consultation Services of University X.

Separate meetings were also arranged with five honours level audit students in the SAIPA (South African Institute of Professional Accountants) programme at University X, representing a wide range of demographical backgrounds. Honours audit students in the SAIPA programme were selected for this purpose because they should be on the same knowledge and competence level of the third-year audit students in the CA programme at University X at the time the study was conducted. The reason is that the third-year CA programme's curriculum is followed in the SAIPA honours year and these students should be able to identify any interpretation issues that might occur when the questionnaires are completed by the third-year audit students of the respective CA programmes of the participating universities. At this meeting the questionnaires were discussed with these students to determine whether they understood each question as intended by the author. A few alterations to clarify the questions were made based on the feedback from the SAIPA students before the pre-test and post-test questionnaires were distributed to the students involved in the experiment.

The reliability and validity of the questionnaires were confirmed by an exploratory principal components factor analysis on each group of questions in the pre-test questionnaire using IBM SPSS (SPSS 2011). The latter was conducted to confirm whether the questions in the questionnaire on each competency identified in the competency framework, measured the same construct. In confirming the factorability of the data, the following measures suggested by Pallant (2013:190) were applied to the questionnaire:

- Kaiser-Meyer-Olkin Measure of Sampling Adequacy (KMO), which suggests a minimum value of 0.6 for a worthy factor analysis; and
- Bartlett's Test of Sphericity (BTS), which suggests a significance value of $p < 0.05$ for the factor analysis to be appropriate.

After confirming the factorability of the data, the questions subject to factor analysis were reduced into the 19 components (competencies) based on the various competency requirements. These competencies (components) included the following (SAICA 2010):

1 Analysing, evaluating and advising on assurance needs.
2 Identifying and considering issues related to accepting an engagement.
3 Establishing the terms of the engagement.
4 Evaluating and assessing the key risks on the performance of the engagement.
5 Determining which rules, standards or policies are to apply to the subject matter being evaluated.
6 Developing materiality guidelines to inform the direction and extent of assurance work, based on the scope and expectations of the engagement.
7 Designing effective and efficient procedures based on the engagement's scope and the assessed risks.
8 Executing the work plan.
9 Documenting the results of procedures performed.
10 Evaluating the evidence and drawing conclusions.
11 Drafting the report upon completion of the engagement.
12 Preparing information for meetings with stake-holders.

13 Identifying and evaluating the risks pertaining to the financial information system.
14 Identifying and documenting the key internal controls (including IT-related controls) implemented in an entity.
15 Evaluating internal control.
16 Designing, implementing and managing the quality control system in the firm.
17 Ethical behaviour and professionalism.
18 Personal attributes.
19 Professional skills.

Table 3 illustrates the results of the exploratory factor analysis confirming the factorability of the data obtained from the pre-test questionnaire as well as the results on the construct validity and the reliability which is measured by the Cronbach alpha coefficient.

Table 3: Reliability and construct validity of the pre-test questionnaire

C*	KMO[1]	BTS	Percentage of variance explained by first factor	Range of question communalities	Cronbach alpha	Average inter-item correlation
1	.886	.000	55.62%	.637–.745	.911	.505
2	.761	.000	55.94%	.520–.597	.842	.470
3	.739	.000	64.90%	.503–.722	.812	.529
4	.937	.000	58.42%	.435–.747	.941	.547
5	.729	.000	77.27%	.744–.795	.852	.659
6	.845	.000	68.53%	.535–.789	.883	.601
7	.785	.000	71.91%	.596–.776	.870	.626
8	.937	.000	60.61%	.316–.742	.949	.569
9	.860	.000	74.46%	.608–.818	.913	.679
10	.942	.000	54.83%	.576–.870	.956	.523
11	.699	.000	80.41%	.699–.865	.876	.704
12	.865	.000	71.01%	.528–.789	.931	.659
13	.500[1]	.000	77.28%	.773	.706	.546
14	.937	.000	57.28%	.520–.775	.937	.535
15	.866	.000	61.02%	.400–.730	.890	.540
16	.719	.000	74.43%	.728–.734	.828	.616
17	.952	.000	73.17%	.298–.839	.953	.690
18	.944	.000	69.03%	.595–.761	.955	.658
19	.965	.000	61.01%	.579–.775	.978	.595

** Competency (component)*

[1]The KMO for this grouping was below the recommended level of 0.6, but the BTS was below the significance value of p < 0.05 by reporting a p = 0.00 and only one factor was extracted in the exploratory factor analysis with the percentage of variance explained by the first factor being 77.28%. Furthermore, this competency only consisted of two questions. Based on these findings, the fact that all the other factors indicated a KMO value of more than 0.6, a BTS significance value of p < 0.05 and the fact that no item had a low correlation (< 0.3) with the total, caused the author to deem the data appropriate for factor analysis.

From Table 3 it can be concluded that the pre-test questionnaire is reliable as the Cronbach alpha coefficient ranged between 0.706 and 0.978 for all competencies and, therefore, met the minimum required level of 0.70 (Delport, De Vos, Fouché, & Strydom 2013:177; Peterson 1994:382; Van der Merwe 2013:116). The construct validity of the pre-test questionnaire is also confirmed due to the fact that:

- The average inter-item correlations were larger than 0.15.
- The percentage of the variance explained by the first factor was more than 50% in all circumstances.
- The screen test confirmed that only one factor is appropriate in all circumstances.
- Only one question reported a slightly lower communality (0.298) than the recommended minimum communality level of 0.3 as suggested by Pallant (2013:206).

Based on these findings which prove the reliability and construct validity of the pre-test questionnaire, the same questionnaire was adopted for the post-test, except for the attitude measure added, as discussed earlier. The results of the simulation evaluation are discussed below.

8 EMPIRICAL RESEARCH FINDINGS

As stated earlier, a quasi-experimental (pre-test/post-test) design was followed in determining whether the newly developed audit simulation had any effect on the audit students' perceived broad competence. In doing so, the following steps were taken in following the quasi-experimental (pre-test/post-test) research design:

- Step 1: Testing differences between the mean scores of University X and University Y for the pre-test.
- Step 2: Movement in mean scores between the pre-test and post-test for both University X and University Y.
- Step 3: Testing differences between the mean scores of University X and University Y for the post-test.

In Step 1 and Step 3, an independent sample t-test was performed. Step 2 consisted of performing a paired sample t-test that measures the movement in mean scores between the pre-test and post-test by only taking into account students who completed both the pre-test and post-test questionnaires. In Step 1 and 3, Levene's test was also performed and in cases

where the assumption of homogeneity of variances was violated (Sig ≤ 0.05), the Sig values which compensate for the violation were reported as proposed by Pallant (2013:250). Because of the non-random sample of the respondents, the results of all the t-tests are interpreted based on effect sizes (*d*), which indicates practical significance (Van der Merwe 2013:98), instead of the Sig (*p)* values, which reveals statistical significance and is disclosed for completeness purposes only.

Ellis and Steyn (2003:52) suggested that *d* should be calculated as the mean difference divided by the maximum standard deviation of the two mean groups that are compared, and that the effect size of *d* should be interpreted as small, where $d = 0.2$; medium, where $d = 0.5$; and large, where $d \geq 0.8$ (also practically significant). The results of the statistical analysis in each step is provided below.

8.1 Testing differences between the mean scores of University X and University Y for the pre-test (Step 1)

Step 1 is required to determine whether there are any statistically and practically significant differences between the mean scores of the students at University X and University Y to ensure that the pre-test results could be compared to the post-test results (Jamieson 2004:277). It could be inferred from Table 4 that the majority of the competencies reported statistically significant differences ($p \leq 0.05$), when random sampling is assumed (Pallant 2013:250), between the mean scores of University X and University Y. These competencies also reported effect sizes (*d*) that ranged between 0.55 and 0.02, which indicate that there is a medium to small practical effect on the mean score differences between University X and University Y. Before the post-test results were compared between the two universities (step 3), these differences were accounted for by performing an analysis of the covariance (ANCOVA), which corrects any differences in the mean scores of the two groups in the pre-test mean scores (Jamieson 2004:277). By doing so, the author ensured that the post-test results could be compared between the two universities (Jamieson 2004:277) and one could subsequently determine whether the simulation project had any effect on audit students' perceived broad competence.

Table 4: Testing differences between the means of University X and University Y for the pre-test

C*	Mean per university		Sig	T-tests		
	University X	University Y		*t* value	*p* value	*d* value
1	3.10	3.18	.017	–1.26	.207	.10
2	3.67	3.73	.995	–.97	.331	.08
3	3.99	3.65	.264	4.94	.000	.42
4	3.52	3.52	.099	.4	.969	.00
5	3.15	3.20	.708	–.70	.484	.06
6	3.43	3.41	.675	.24	.809	.02
7	3.15	2.98	.631	2.35	.019	.20
8	3.07	2.62	.617	6.32	.000	.55
9	3.15	2.83	.710	4.12	.000	.36
10	3.05	2.67	.671	5.55	.000	.48
11	2.95	2.58	.092	4.49	.000	.38
12	3.15	2.82	.983	4.31	.000	.38
13	3.55	3.52	.278	.33	.743	.03
14	3.59	3.43	.249	2.65	.008	.23
15	3.36	3.32	.557	.70	.485	.06
16	3.15	2.88	.444	3.43	.001	.29
17	4.19	3.98	.351	3.30	.001	.27
18	4.03	3.65	.016	5.26	.000	.44
19	3.69	3.35	.509	4.97	.000	.41

**Competency (component)*

8.2 Movement in mean scores between the pre-test and post-test for both University X and University Y (Step 2)

In this section, the movement will be discussed in the mean scores between the pre-test and post-test for both University X and University Y respectively. The results of the paired sample t-test are stated by discussing the results of the one question in the questionnaire (Question 7) that was not subject to factor analysis, followed by the competencies supported and informed by the subject content and audit process related to auditing and assurance as well as generic and pervasive skills.

It may be noted from Table 5 that the students at University X indicated a statistically significant increase ($p \leq 0.05$) as well as a significant increase of a medium effect size ((*d*) with $d = 0.52$) in the students' understanding of the audit process as a whole after the students participated in the newly developed audit simulation. Moreover, it is noted that all the competencies indicated a statistically significant increase ($p \leq 0.05$) in the perceived competence level of the students after the students participated in the newly developed audit simulation. Furthermore, the perceived competence level of the students after completion of the audit simulation also increased significantly for almost half (9) of the competencies ($d \geq 0.8$), with certain competencies indicating a medium to small significant increase in the perceived competence levels, with effect sizes ranging between $d = 0.21$ and $d = 1.18$.

Table 5: Movement in mean scores between the pre-test and post-test for University X

C*	N	Mean scores		Std. deviation		*p* value	*d* value
		Pre-test	Post-test	Pre-test	Post-test		
Q7	279	3.63	4.08	.845	.781	.000	0.52
1	279	3.08	3.78	.743	.810	.000	0.94
2	279	3.67	4.01	.726	.725	.000	0.46
3	279	3.99	4.17	.765	.760	.001	0.23
4	279	3.50	3.99	.739	.725	.000	0.66
5	279	3.11	3.94	.854	.801	.000	0.98
6	279	3.41	3.98	.815	.798	.000	0.70
7	279	3.12	3.88	.820	.799	.000	0.92
8	279	3.03	3.90	.769	.788	.000	1.13
9	279	3.12	3.99	.874	.805	.000	1.00
10	279	3.01	3.92	.767	.768	.000	1.18
11	279	2.91	3.90	.862	.890	.000	1.15
12	279	3.12	4.00	.852	.804	.000	1.03
13	279	3.54	4.04	.821	.741	.000	0.61
14	279	3.57	4.02	.714	.736	.000	0.63
15	279	3.35	3.91	.730	.746	.000	0.77
16	279	3.11	3.90	.850	.822	.000	0.93
17	278	4.18	4.33	.715	.749	.003	0.21
18	278	4.02	4.33	.762	.727	.000	0.41
19	278	3.67	4.22	.741	.736	.000	0.73

**Competency (component)*

Based on these findings it can be concluded that the students' perceived competence levels increased, and almost half (9) of the competencies increased significantly from before the audit simulation to after performing the audit simulation, with only three out of the 19 competencies showing a minute increase in perceived competence level. Hence, the audit simulation had a significant positive effect on almost half (9) of the competencies and an overall positive effect on all the competencies. The movement in the mean scores between the pre-test and post-test for University Y is discussed next.

Table 6: Movement in mean scores between the pre-test and post-test for University Y

C*	N	Mean scores		Std. deviation		*p* value	*d* value
		Pre-test	Post-test	Pre-test	Post-test		
Q7	133	3.53	3.67	.754	.756	.007	0.18
1	133	3.20	3.32	.509	.621	.025	0.24
2	133	3.72	3.66	.713	.669	.322	0.08
3	133	3.63	3.61	.793	.719	.777	0.02
4	133	3.55	3.67	.598	.630	.032	0.21
5	133	3.20	3.20	.783	.846	.221	0.13
6	133	3.42	3.82	.725	.748	.000	0.55
7	133	2.97	3.13	.785	.790	.055	0.20
8	133	2.60	3.20	.734	.639	.000	0.82
9	133	2.82	3.14	.833	.828	.000	0.38
10	133	2.64	3.18	.698	.655	.000	0.78
11	133	2.58	3.05	.892	.779	.000	0.52
12	133	2.81	3.12	.725	.765	.000	0.43
13	133	3.55	3.65	.809	.873	.233	0.13
14	133	3.46	3.48	.589	.638	.834	0.02
15	133	3.37	3.39	.567	.688	.705	0.04
16	133	2.84	3.19	.842	.775	.000	0.41
17	133	4.04	3.97	.699	.687	.273	0.11
18	133	3.80	3.78	.741	.743	.710	0.03
19	133	3.42	3.43	.667	.664	.892	0.01

**Competency (component)*

From Table 6 it can be deducted that the students at University Y demonstrated a significant increase ($p \leq 0.05$) in their understanding of the audit process as a whole after the students continued with normal lectures during the experiential period. Although this increase is statistically significant, the effect size (d) was small, with $d = 0.18$. Furthermore, it is noted that only 10 out of the 19 competencies revealed a statistically significant increase ($p \leq 0.05$) in the perceived competence level, and of these only four competencies revealed a medium to practically significant (d) increase in the perceived competence levels with effect sizes ranging between $d = 0.52$ and $d = 0.82$. Although the other competencies revealed an increase in the perceived competence level, none of these were statistically or practically noteworthy. Based on these findings it can be concluded that the students' perceived competence levels in certain instances increased significantly with only one practical significant increase noted by attending the normal lectures during the experiential period.

Now that the movement in the mean scores between the pre-test and post-test for both University X and University Y have been discussed, the next step is to determine the differences between the mean scores of University X and University Y for the post-test in order to determine the significance of the effect that the simulation project had, if any, on audit students' perceived broad competence.

8.3 Testing differences between the mean scores of University X and University Y for the post-test (Step 3)

In testing the differences between the mean scores of University X and University Y for the post-test, the author was able to determine whether the simulation project had any effect on audit students' perceived broad competence and whether the audit simulation had a greater effect on the audit students' perceived broad competence than just attending normal lectures (passive approach) in the audit subject. As noted earlier, this was undertaken by performing an independent sample t-test between the adjusted mean scores from the post-test, after the mean scores obtained in the post-test were corrected for any differences in the pre-test mean scores between University X and University Y by performing an analysis of the covariance (ANCOVA) as discussed in the results of Step 1. The latter is necessary to ensure that the results of the pre-test could be compared to the post-test. Table 7 illustrates these results. The following is noted from the results outlined in Table 7:

- a statistically significant difference was found to exist ($p \leq 0.05$) between the adjusted mean scores of University X and University Y, for the students' understanding of the audit process as a whole as well as for all the competencies tested in this study; and
- all the competencies except for the students' perceived competence to develop materiality guidelines to inform the direction and extent of assurance work, based on the scope and expectations of the engagement ($d = 0.22$) and ethical behaviour and professionalism ($d = 0.45$), indicated a medium to practically significant difference in the adjusted mean scores of University X and University Y with d ranging between 0.52 and 1.05. The difference between the adjusted mean scores of University X and University Y for an understanding of the whole audit process also indicated a significant difference of medium practicality, with $d = 0.51$.

Table 7: Testing differences between the mean scores of University X and University Y for the post-test

C*	Adjusted means per university		Mean square	*p* value	*d* value
	University X	University Y			
Q7	4.07	3.69	0.540	.000	0.51
1	3.79	3.29	0.465	.000	0.75
2	4.01	3.65	0.432	.000	0.55
3	4.12	3.71	0.462	.000	0.61
4	3.99	3.66	0.398	.000	0.53
5	3.95	3.28	0.608	.000	0.86
6	3.98	3.82	0.532	.040	0.22
7	3.86	3.16	0.581	.000	0.93
8	3.86	3.29	0.500	.000	0.80
9	3.97	3.19	0.616	.000	0.99
10	3.88	3.26	0.486	.000	0.88
11	3.87	3.10	0.695	.000	0.93
12	3.98	3.17	0.602	.000	1.05
13	4.04	3.65	0.551	.000	0.52
14	4.01	3.51	0.422	.000	0.77
15	3.91	3.39	0.454	.000	0.78
16	3.87	3.25	0.573	.000	0.83
17	4.31	4.00	0.460	.000	0.45
18	4.31	3.83	0.467	.000	0.71
19	4.19	3.49	0.455	.000	1.04

**Competency (component)*

Based on these findings, it can be concluded that the newly developed audit simulation had a greater effect on the audit students' perceived broad competence (i.e. auditing and assurance as well as generic and pervasive skills) and the audit students' understanding of the audit process as a whole (i.e. increasing their perceived broad competence) in relation to just attending normal lectures in the audit subject. Therefore, this finding supports the results of researchers such as Steenkamp and Rudman (2007: 23), Hosal-Akman and Simga-Mugan (2010:251), as well as Steenkamp and Von Wielligh (2011:9), noted earlier, who reported that courses in accounting degrees frequently apply out-dated methods and follow a passive learning approach. The students are required to sit down in a classroom and no active participation is required of them in the learning process.

The fact that the audit simulation had a greater effect on the students' perceived competence levels than the students that just had normal lectures (passive approach) during the experiential period, also confirms the argument put forward by Siegel *et al* (1997:218) in the late 1990s. These researchers stated that by

following a passive technique of conveying auditing theory to the untried young auditor in the making, yields poor results when their audit knowledge is examined. Although the student's perceptions have been obtained in this study, and not physical marks, the results show a deficiency in their perceived competence upon self-examination. Furthermore, the latter also supports the problem statement of this study which noted that the approach followed to date, in preparing audit students at higher education level for the actual auditing environment that they will form part of, is still in need of change. This is because the students taught by means of a passive approach indicated a lower perceived competence level than the students who formed part of the experimental group and who were taught by actively involving them in the learning process (active approach). Hence, the implementation of simulations, such as the one tested in this study, may assist in bringing the required change to the audit classroom and audit education in general.

8.4 Evaluation of the simulation

As noted earlier, the last section in the post-test questionnaire included questions on the audit students' attitude towards the audit simulation (Question 178 to 186). The scale ranged from 1 (extremely negative) to 5 (extremely positive). A neutral feeling was expressed by 3. This part of the questionnaire was only completed by the students at University X who participated in the experimental design and completed the audit simulation.

From Table 8 below it can be deducted that the students' attitude towards the audit simulation was generally positive, with all mean scores greater than 3.00. The students' attitudes towards the audit simulation that were most positive were that of good (M = 3.91), comfortable (M = 3.82), fresh (M = 3.81) and understandable (M = 82). Other less positive attitudes, but still leaning towards the positive, revealed that students felt that the audit simulation was an exciting (M = 3.63) and pleasant (M = 3.69) experience which may have contributed to the students' positive attitude towards the audit simulation by indicating that it is likeable (M = 3.74) and it brought a sense of happiness (M = 3.74) and calmness (M = 3.74) whilst participating in the audit simulation.

Table 8: Attitude towards the audit simulation

Question	Description[1]	Range	N	Mean
178	Unlikeable / Likeable	1 (Negative) to 5 (Positive)	304	3.74
179	Poor / Good	1 (Negative) to 5 (Positive)	304	3.91
180	Unhappy / Happy	1 (Negative) to 5 (Positive)	304	3.74
181	Uncomfortable / Comfortable	1 (Negative) to 5 (Positive)	304	3.82
182	Tense / Calm	1 (Negative) to 5 (Positive)	304	3.74
183	Dull / Exciting	1 (Negative) to 5 (Positive)	304	3.63
184	Suffocating / Fresh	1 (Negative) to 5 (Positive)	304	3.81
185	Unpleasant / Pleasant	1 (Negative) to 5 (Positive)	304	3.69
186	Confused / Understandable	1 (Negative) to 5 (Positive)	304	3.82

[1] *Items form part of Kay's Computer Attitude Measure as used by Noyes and Garland (2005:238 – adapted), Fouché (2006:183 – adapted) and Van der Merwe (2013:152 – adapted).*

9 CONCLUSION

The objective of this study was to evaluate whether a newly developed audit simulation would assist in enhancing audit students' perceived broad competence. Based on the findings it can be concluded that the audit simulation had:

- a positive effect on the audit students' perceived competence levels in audit and assurance as well as the various generic and pervasive skills, with almost half (9) of the competencies indicating a practically significant increase ($d \geq 0.8$), as well as a medium to small significant increase in the perceived competence levels, with effect sizes ranging between d = 0.21 and d = 1.18, thus enhancing audit students' perceived broad competence;
- a greater effect on audit students' perceived broad competence and audit students' understanding of the audit process as a whole in relation to attending normal lectures in the audit subject, with only two competencies indicating a lower than medium practical significance (d = 0.5); and
- A positive impact on the students' attitude since all the attitude measures applied in this study leaned towards the positive.

It was, therefore, proven in this study that this newly developed audit simulation can assist in providing the change that is required in how accounting educators develop and train the young auditors of the future. Furthermore, particularly in South Africa, it also proved to be a tool that audit educators can use to assist students to develop the several competencies in auditing and assurance as well as the generic and pervasive skills required by the SAICA competency framework.

The empirical findings of this study have also proven that there is still a real need for change in the manner auditing is taught at universities and other institutions of higher learning. This finding is specifically noteworthy in the South African context because students from two SAICA-accredited universities participated in this study. This fact also increases the generalisability of the results of the study as they are not confined to one university. Finally, it can be concluded that by applying teaching methodologies, such as this newly developed audit simulation, certain required change can be brought to the audit education environment.

10 RECOMMENDATIONS AND AREAS FOR FURTHER RESEARCH

Based on the findings of this study, it is recommended that audit lecturers should attempt to apply a teaching methodology that actively involves students in the learning process as well as give students the opportunity to develop the various skills required when they start their professional careers after graduation.

In the South African context, this could include, but is not limited to, the use of more active learning tools such as simulations and integrated case studies that specifically include the SAICA competencies to be achieved. The latter should also be used to assess whether the students have developed the competencies required of students when they enter practice after completion of their tertiary studies. By using such instruments not only as a teaching tool, but also as a method of assessment, the criticism against the method of examination, where students are assessed on their competence by means of a written examination, can also be addressed to a certain extent.

Although these recommendations may not fully address all the issues that the audit pedagogy is facing, audit lecturers can address these problems and make a meaningful contribution to the learning experience of students by actively involving them in the learning process. By doing this the auditing profession's call for students to be more actively involved in the process of developing the necessary skills and knowledge to be able to conduct an audit in terms of the ISAs can also be addressed.

Several other possibilities for further research exist which include expanding the study to all SAICA-accredited universities so as to corroborate or disprove the findings of this study. This may lend itself to forming a theory of the best approaches to teach auditing at the higher education level. Furthermore, the effect of the newly developed audit simulation on students' auditing marks could also be tested. Further development opportunities also exist and include modifying the newly developed questionnaire so as to include the competencies and subject content requirements of all the disciplines in the accounting pedagogy, granting lecturers the opportunity to assess their teaching methodology across several subject and academic year groups. Finally, the audit simulation could be developed further into a digitally based teaching tool so as to limit costs to students as well as to make it more accessible to the broader populations of students and lecturers around the world.

11 LIMITATIONS OF THE STUDY

Although this study has highlighted that this newly developed audit simulation can assist in answering the call for change in audit education, the findings of this study are not without limitations. The author acknowledges the following limitations, although attempts were made to address these, which was evident throughout the research:

- The results of the quantitative analysis may be limited with regard to its generalisability due to the non-random sampling applied.
- The sample population consisted of students studying at two different SAICA-accredited universities with certain differences in demographical backgrounds.
- The experimental design tested students' perceptions of the effectiveness of the audit simulation and not actual measures such as their marks.

REFERENCES

Arens, A.A., May, R.G. & Dominiak, G. 1970. A simulated case for audit education. *Accounting Review*, 45(3):573-578.

Bagley, P.L. & Harp, N.L. 2012. Shoe Zoo, Inc.: A practice in electronic work papers, tick mark preparation, and client communication through the audit of property, plant and equipment. *Issues in Accounting Education*, 27(4):1131-1151.

Barac, K. 2012. Learning approaches to the study of auditing followed by prospective South African chartered accountants. *Southern African Business Review*, 16(2):47-68.

Barkman, A.I. 1998. The use of live cases in the accounting information systems course. *Journal of Accounting Education*, 16(3/4):517-524.

Blair, E.A., Blair, J. & Czaja, R.F. 2014. *Designing surveys*: *A guide to decisions and procedures*. 3rd edition. London: Sage.

Borthick, A.F. & Curtis, M.B. 2004. Audit simulation for due diligence on fast-fashion inventory through data querying. [Online]. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1. 126.4817&rep=rep1&type=pdf. (Accessed: 3 March 2014).

Botha, W.J.J. 2001. Pre-qualification education of registered accountants and auditors in South Africa: Perspectives on whether the education process is normatively justifiable. *Meditari Accountancy Research*, 9(1):33-59.

Chung, K.H., Shin, J.I., Oh, J.S. & Lee, C.W. 2013. The effect of site quality in repurchase intention in internet shopping through mediating variables: The case of university students in South Korea. *International Journal of Information Management*, 33:453-463.

Creswell, J.W. 2005. *Educational research*. New York: Pearson.

De Lange, P., Jackling, B. & Gut, A.M. 2006. Accounting graduates' perceptions of skills emphasis in undergraduate courses: An investigation from two Victorian universities. *Accounting and Finance*, 46:365-386.

Delport, R.C.S.L., De Vos, E.A., Fouché, C.B. & Strydom, H. 2013. *Research at grass roots: For the social science and human services profession.* Pretoria: Van Schaik.

Ellis, S.M. & Steyn, H.S. 2003. Practical significance (effect sizes) versus or in combination with statistical significance (p-values). *Management Dynamics*, 12(4):51-53.

Fouché, J.P. 2006. Program development for first year accounting in South African higher education. (PhD thesis, North-West University, Potchefstroom).

Gawe, N., Jacobs, M. & Vakalisa, N.C.G. 2012. *Teaching learning dynamics*. 4th edition. Cape Town: Pearson.

Gelinas, U.J., Levy, E.S. & Thibodeau, J.C. 2001. Norwood Office Supplies Inc.: A teaching case to integrate computer-assisted auditing techniques into the auditing course. *Issues in Accounting Education*, 16(4):603-638.

Hosal-Akman, N. & Simga-Mugan, C. 2010. An assessment of the effects of teaching methods on academic performance of students in accounting courses. *Innovations in Education and Teaching International*, 47(3):251-260.

Jamieson, J. 2004. Analysis of covariance (ANCOVA) with different scores. *International Journal of Psychophysiology*, 52:277-283.

Jeffries, P.R. 2005. A framework for designing, implementing and evaluating simulation used as teaching strategies in nursing. *Nursing Education Perspectives*, 26(2):96-103.

Krogstad, J.L., Smith, G. & Clay, R.J. 1986. Impact of a simulation of audit practice. *Issues in Accounting Education*, 1(2):309-320.

Lasley, T.J. & Ornstein, A.C. 2004. *Strategies for effective teaching*. 4th edition. New York: McGraw-Hill.

McKerchar, M. 2008. Philosophical paradigms, inquiry strategies and knowledge claims: Applying the principles of research design and conduct to taxation. *E-journal of Tax Research*, 6(1):5-22.

Miller, C.R. & Savage, A. 2009. Vouch and trace: A revue recognition audit simulation. *Issues in Accounting Education*, 24(1):93-103.

Noyes, J. & Garland, K. 2005. Students' attitudes towards books and computers. *Computers in Human Behaviour*, 21(2):233-241.

Olivier, M. 2014. Influence: SAICA response to a Finweek opinion piece. *Accountancy SA*. [Online]. http://www.accountancysa.org.za/influence-saica-response-to-a-finweek-opinion-iece/ (Accessed: 23 July 2014).

Pallant, J. 2013. *SPSS survival manual*. 5th edition. Berkshire, UK: McGraw-Hill Open University Press.

Peterson, R.A. 1994. A meta-analysis of Cronbach's coefficient alpha. *Journal of Consumer Research*, 21(2):381-391.

SAICA (South African Institute of Chartered Accountants). 2010. *Competency framework detailed guidance for academic programmes: Competencies of a CA (SA) at the point of the part I examination (assessment of core technical competence).* Johannesburg: SAICA.

Saunders, M. & Machell, J. 2000. Understanding emerging trends in higher education curricula and work connections. *Higher Education Policy*, 13:287-302.

Siegel, P.H., Omer, K. & Agrawal, S.P. 1997. Video simulation of an audit: An experiment in experiential learning theory. *Accounting Education*, 6(3):217-230.

SPSS Statistics. 2011. Rel. 20.0.0. IBM Corporation.

Steenkamp, L.P. & Rudman, R.J. 2007. South African students' perceptions of the usefulness of an audit simulation. *Meditari Accountancy Research*, 15(2):23-41.

Steenkamp, L.P. & Von Wielligh, S.P.J. 2011. The perceptions of accounting students of the usefulness of an audit simulation at university level. *Southern African Journal of Accountability and Auditing Research*, 11:9-21.

Tan, L.M., Fowler, M.B. & Hawkes, L. 2004. Management accounting curricula: Striking a balance between the views of educators and practitioners. *Accounting Education*, 13(1):51-67.

Tonge, R. & Willett, C. 2012. An audit learning experience: A pilot project through cooperation with a third sector organization. *Accounting Education: An International Journal*, 21(2):171-185.

Ulrich, T.A., Michenzi, A.R. & Blouch, W.E. 2011. Assessing curricular design. ASBBS Annual Conference, Las Vegas, Nevada, February, 2011.

Van der Merwe, N. 2013. Ameliorating chartered accountants' training at a South African university: Interventions for reform. (PhD thesis, North-West University, Potchefstroom).

Walgenbach, P.H. & Frank, W.G. 1971. A simulation model for applying audit-sampling techniques. *Accounting Review*, 46(3):283-588.

Weber, R. 1978. Auditor decision making on overall systems reliability: Accuracy, consensus, and the usefulness of a simulation decision aid. *Journal of Accounting Research*, 16(2):368-388.

Worrell, J.L. 2010. Blazer communication: A procurement audit simulation. *Issues in Accounting Education*, 25(3):527-546.

Audit committees' communication on internal audit to boards of directors

K Barac

Department of Auditing
University of Pretoria

G Williams

Department of Auditing
University of Pretoria

ABSTRACT

Audit committees are expected to communicate effectively as trusted relationships are created when high quality communication takes place. Very little research has been performed on communication between audit committees and boards of directors and no studies have been performed on audit committees' communication of internal audit information to boards of directors. In closing the gap this article examines the effectiveness of the process of communicating internal audit information between the audit committee and the board, and is useful as previous audit committee studies focussed predominantly on the diligence, resources, authority, and composition of the audit committee and not on the actual process of communication. A case study of three JSE listed mining companies operating in the South African gold, platinum, coal and energy sectors was performed to understand whether communication processes between their audit committees and boards of directors were effective. This involved understanding the views of the chairpersons of the audit committee and board, non-executive directors and chief audit executives for the three companies concerned, because these parties are important role players in communicating internal audit information between their corresponding committees. The findings of the study identified strengths and weaknesses of internal audit information to be communicated and considered the communication process. Barriers, such as board dynamics, culture and language, and the conduct of members were identified. The study showed the importance of the role of the chairperson of the audit committee to promote effective communication and to fulfil such a role, identified attributes are needed.

Key words

Internal audit; audit committees; board of directors; communication; mining; South Africa; internal audit function; chairperson of the audit committee; communication process; effective communication

1 INTRODUCTION

The 2008 financial crises and recent worldwide corporate failures have brought into stark relief the efficacy of audit committees (Aldamen, Duncan, Kelly, McNamara & Nagel 2012). As a statutory committee, the audit committee is task with an "oversight role to assist directors in meeting their financial reporting, risk management and control- and audit related responsibilities" (Marx 2009:33). Risks related to safety, labour and community relations, social development, transformation and environmental impacts make up a significant portion of risk profiles of mining companies such as Lonmin Plc (2013). The tragic event on 16th August 2012 when 36 Lonmin Plc employees were killed and 78 wounded by police officers during the Marikana miners' strike (Twala, 2012) casts doubt on the efficacy of the company's risk management process. It raises the question whether such failures of risk management was found in audit committee communications to the board of directors.

The audit committee has a duty to effectively communicate internal audit information to the board (IoD 2009). High quality communication creates trusted relationships between the internal audit function (IAF), the audit committee and the board (Abdolmohammadi, Ramamoorti, & Sarens, 2013: xi). Studies, however, have raised concerns about the effectiveness of audit committee communication (Turley & Zaman 2007; Cohen, Krishnamoorthy & Wright 2002).

This research article examines the effectiveness of the process of communicating internal audit information between the audit committee and the board. It adds to the current knowledge on communication between boards and audit committees because previous studies considering audit committee reporting focussed on the composition, authority, resources and the diligence of the audit committee and not on the communication process itself (Barua, Rama & Sharma 2010; Abbott, Parker & Peters 2004; DeZoort, Hermanson, Archambeault & Reed 2002). The literature on how an audit committee should effectively communicate internal audit information to the board remains scant, but drawing on communication literature such communication should build rapport, share strategic goals, clarrify assumptions and build

trust by the congruency with word and action (Adler, 2012; Colquitt, Scott, & LePine 2007; Hubbard 2000).

The remainder of this article is organised as follows: the next section presents the objectives, significance, and limitations underpinning the study. The sections that follow describe the theoretical background of the article, the methodology applied, and the findings and deductions. Conclusions drawn from the study and areas identified for future research are presented in the final section.

2 OBJECTIVE, SIGNIFICANCE AND LIMITATIONS

The objective of this study is to examine the effectiveness of the communication process between audit committees and their boards on internal audit information at three mining companies listed on the Johannesburg Stock Exchange (JSE).

There is anecdotal evidence that internal audit information may be omitted, diluted or misrepresented to the board due to a variety of reasons. One such reason postulated is that members of the audit committees may not have the knowledge of internal audit theory and practice to effectively provide such information to the board. As a consequence; there is a concern that the board may not optimise the resource of internal audit information and act upon its findings and recommendations (Paterakis & Cefaratti 2014; Drent 2002). As there is limited research into the communication process on internal audit information between the audit committee and its board and as the aforementioned perceptions have not been investigated the findings of this study add a pragmatic perspective.

The findings of the study could provide audit committees and boards with guidance on how to improve procedures to ensure complete, accurate and useful communication protocols on internal audit information. IAFs could become aware of how their information is being communicated by audit committees to boards, knowledge which may impact on their reporting processes. The internal audit profession could benefit through informed guidance by the Institute of Internal Auditors (IIA) on how internal audit information should be presented to audit committees to promote effective communication when such information is shared with boards.

3 LITERATURE REVIEW

An increasing number of overseas earnings restatements along with accusations of financial statement fraud by companies like Enron, Parmalat, WorldCom, Adelphia, and Global Crossing have damaged public confidence in corporate governance (Kirkpatrick 2009; Melis 2005; Clarke 2004). This has spurred discussion on whether the communication of audit committee information between audit committees and boards of directors is effective (Paterakis & Cefaratti 2014; Rezaee, Olibe, & Minmier 2003).

In terms of laws and regulations, certain boards of director functions are delegated to well-structured committees without renouncing their responsibilities (Lenz & Sarens 2012; Marx & Voogt 2010; Charan 2005; DeZoort *et al* 2002). One such committee is the audit committee and together with the board, they are important governance role players (Coetzee & Fourie 2009; Davies 2008; Charan 2005). Mallin (2003) believes the audit committee has become the most significant sub-committee of the board of directors.

Audit committees are well established in South Africa (Marx & Voogt 2010; Marx 2009; Van der Nest 2008). Together with the Companies Act 71 of 2008 that incorporates into statute issues of corporate governance, the King Reports (IoDSA 1994; 2002; 2009; RSA 2009) set out the duties and responsibilities of an audit committee (King 2010). These include traditional responsibilities of overseeing external audit, financial reporting, internal control and risk management together with emerging issues such as sustainability reporting and ethics compliance (Marx 2009). In terms of the draft King IV Report (IoDSA 2016), an audit committee should provide independent oversight of audit and assurance requirements, independence of the auditor and other assurance providers in the combined assurance model (including internal audit), audit quality and integrity or reliability and usefulness of reports.

A well-functioning audit committee and IAF are the primary mechanisms to limit agency risk due to their importance in the corporate governance mosaic (Eulerich, Theis, Velte & Stigtbauer 2013; Davies 2008; Cohen, Gaynor, Krishnamoorthy & Wright 2007; Abbott & Parker 2000). Due to the separation of management and ownership, shareholders require protection as management does not always behave in the best interest of shareholders (Abbott & Parker 2000; Fama & Jensen 1983; Jensen & Meckling 1976). Non-executive directors are at a disadvantage as they suffer from asymmetrical knowledge in contrast with executive directors who have a deep understanding of the business through their direct involvement (King 2006; Adamsb1994; Watts & Zimmerman 1983). In this regard agency costs are incurred which leads to monitoring mechanisms such as the use of internal audit and an audit committee (Goodwin-Stewart & Kent 2006; Adams 1994). Both these mechanisms rely on effective communication processes (King 2006:70-71) as the audit committee is required to effectively communicate internal audit information to the board (IoD 2009).

The 2008 financial crisis and recent worldwide corporate failures focussed the spot light on what constitutes an effective audit committee and board communication (Paterakis & Cefaratti 2014; Financial Crisis Inquiry Commission 2011). The argument was made that members of audit committees were ill prepared, did not understand, nor communicate the risks assumed to the board (Braiotta, Gazzaway, Colson & Ramamoorti 2010:356). Audit committees report to their boards on various matters. These include commenting on and making submissions on the company's annual financial statements, accounting practices, financial systems of internal controls, reporting, and financial policy (PCAOB 2012; IIA 2011; South Africa 2010; IoD 2009). As such an

audit committee needs to communicate to the board and be their "oversight watchdog" on the process of financial reporting, risk management and internal control to enable them to make informed decisions (Marx & Voogt 2010; Charan 2005:59).

The literature supports the view that good communication to boards enhances the effectiveness of audit committees (Paterakis & Cefaratti 2014; Zaman & Sarens 2013). Effectiveness of audit committees has been widely explored in the literature and relate to its composition (Lary & Taylor 2012; Klein 2002; Archambeault & DeZoort 2001; Beasley & Salterio 2001; Scarborough, Rama & Raghunandan 1998; DeZoort 1997; Kalbers 1992(b), authority, (DeZoort *et al* 2002; Abdolmohammadi & Levy 1992; Kalbers 1992(a); and Kalbers & Fogarty 1993), resources, (De Zoort, Hermanson & Houston 2003; De Zoort *et al* 2002; Raghunandan, Read and Rama 2001; Cohen & Hanno 2000) and the diligence with which audit committee members exercise their duties and responsibilities (DeZoort *et al* 2002; Carcello, Hermanson & Neal 2002; Archambeault & DeZoort 2001; Abbott & Parker 2000; Collier & Gregory 1999). Diligence is regarded as the process interaction of incentive, motivation and perseverance between members to achieve communication effectiveness (DeZoort *et al* 2002). Audit committee effectiveness will be achieved when there are honest and independent members that are financially literate, have the authority of legislation to act, have timely access to management information and communicate well with all relevant role players (DeZoort *et al* 2002).

A review of the literature yields discussion on audit committee communications relating to quality of financial reporting, earnings management, reinstatements and fraudulent financial reporting but little on the benefits of effective communication (Barua *et al* 2010; Abbott *et al* 2004; Klein 2002; Beasley, Carcello, Hermanson & Lapides 2000; Abbott & Parker 2000; Abbott, Park & Parker 2000; DeZoort 1997). Though audit committees have been in existence for many years and there are high expectations on them to deliver, there is little known about their communication effectiveness (Pomeranz 1997). Avison and Cowton (2012) concur and state that compared to the board, little attention has been given to communication between board sub-committees and the board.

Internal audit studies have highlighted the benefits of good communication (Paterakis & Cefaratti 2014). Internal auditors who effectively communicate enlarge their significance to companies and help boards to manage risk (Drent 2002). Open communications with key stakeholders develop an understanding of the internal auditor's role (Paterakis & Cefaratti 2014; Drent 2002). Existing research in the literature offers little insight into operational situations surrounding audit committee activity and its interaction with the board. One study investigated communication between an audit committee, its members, executives, internal auditors and external auditors (Turley & Zaman 2007). The study examined formal and informal processes and power relationships (Turley & Zaman 2007). They found that communication and governance are not improved by a sole reliance on a standardized process, and the audit committee has an influence on the power relationships between company participants (Turley & Zaman 2007).

Although, as indicated above, guidance is provided on what type of internal audit information gets communicated to the board (for example quarterly and annual reports, and audit committee charters) (Spencer-Pickett 2010:960), there is little literature on the interpersonal oral, written and non-verbal interaction between the audit committee and the board and whether the communication was effective (IoD 2009; IIA 2011). Consequently, communication literature is drawn on to determine indicators for effective communications.

Interpersonal communication can be classified as oral, written and non-verbal (Rashotte 2002; Robbins & Judge 2013; Tubbs 2010). Indicators of effective interpersonal communication are rapport, sharing, listening, clarifying, congruency with words and action and empathy (Adler 2012:15; Hubbard 2000). Adler (2012:13-14) explains that the communication process involves a communicator sending a message to a receiver which is encoded, decoded and filtered. By building rapport, the sharing of strategic goals, engaging in active listening, clarifying assumptions, and ensuring congruency of words with body language, effective communication can occur (Adler 2012; Hubbard 2000).

The key to management communication is to elicit action and this involves upward, downward and lateral communication (Robbins & Judge 2013; Siegel & Schultz 2011). There are psychological and physiological filters that cause dysfunctional communications and trait variables need to be considered, such as perception, gender, self-esteem and shyness (Tubbs 2010:37-38). Tubbs (2010:35-65) explains that incorrect perceptions of others causes barriers that could lead to a dysfunctional communication process. Tubbs (2010:62) argues the key to active listening and thus communication is empathy, being aware of the receiver's perceptions. These could be considered by removing gender and cultural barriers in the workplace. The use of gender-neutral terms should be used to prevent offence and language should be free of bias. This requires the avoidance of the use of generic terms and all genders should be addressed equally (Shober 2008:138-139).

Trust is built by congruency with words and action and the characteristics of integrity, benevolence and ability (Colquitt *et al* 2007). As effective communication with action, builds trust and the inverse destroys it. The organizational climate between the audit committee and the board should be trusting and supportive (Puth 2002:46). Clear messages, clarifying assumptions, should be sent. This means that messages verbal and non-verbal should be interesting, organized, purposeful, specific and concise. (Adler 2012:45-56). These would allow boards to elicit action thus constructively using communication (Siegel & Schultz 2011).

The literature supports the view that for communication to be effective it is required to be supported by a process - during and after a meeting

(Tuggle, Schnatterly & Johnson 2010; Romano & Nunamaker 2001; Volkema & Niederman 1996). Planning for effective communication is important. It is important to plan organisational meetings to ensure that human resources invested in such meetings are maximised to produce effective communication and audit committee meeting goal achievement (Volkema & Niederman 1996). Scholars concurred that communication would be effective where meetings are supported by the advanced distribution of agendas and minutes of previous meetings allowing the participants to prepare the necessary in committee questions, purposes are clear and there is widespread attendee participation (Rogelberg, Leach, Warr & Burnfield 2006; Rogelberg, Scott & Kello 2007; Volkema & Niederman 1996). Such pre-meeting documents epitomize a powerful tool for audit committee members.

A process during committee meetings is important to ensure goal clarity, focussed communication and team communication effectiveness (Bang, Fuglesang, Ovesen & Eilertsen 2010). Team effectiveness is positively related with goal clarity and focussed communication and that disharmony and lack of trust between parties causes the inverse. Goals direct attention, effort and action toward goal-relevant actions (Locke & Latham 2006). The chairpersons of both audit and board committees should therefore incalcate at the beginning of a meeting a process of clear meeting goals identification. Important is speaking up during the meeting when a goal or communication is not understood to ensure members remain focussed. Such process will improve task performance, quality of member relationships, audit and board committee member satisfaction and focussed communications (Bang *et al* 2010).

The process of communication does not end after the meeting. To ensure audit committee and board accountability the following six practices will foster effective communication and accountability after the meetings. These are (1) setting clear expectations, (2) developing and using policies regarding conflicts of interest, (3) maintaining effective communications with constituencies, (4) conducting audit committee and (5) board performance assessments and (6) experimenting with new communication methods (Tuggle *et al* 2010; Holland 2002; Romano & Nunamaker 2001).

4 METHODOLOGY AND RESEARCH DESIGN

The objective of this study is to examine the effectiveness of the communication processes between audit committees and their boards on internal audit information at three mining companies listed on the JSE. This involved investigating the perceptions of the chairperson of audit committees (CACs), the chairperson of the boards (BCs), one non-executive director (NED) from each company and the chief audit executives (CAEs) because all these parties are pivotal in communicating internal audit information at and between their respective committees as part of good governance (Paterakis & Cefaratti 2014). In total eleven interviews were held. The mining sector was selected for this study due to its past and present importance to the South African developing economy (Hirsch 2005:20). Also due to the current economic turbulence where a strike in the mining sector negatively impacted on the country's economy (Bisseker 2014). Three mining companies were selected from the JSE which allowed for access to other information (such as board and audit committee minutes) to promote tiangulation opportunities.

The research objective has been reached using qualitative research to examine the effectiveness of the communication process between audit committees and their boards on internal audit information at three mining companies listed on the JSE. It requires a deep understanding of the effectiveness of the communication process on internal audit information (Sekaran & Bougie 2013:336). A case study method was selected as it allows for such an in-depth understanding (Creswell 2009). A limitation of a case study is that the findings cannot be generalised and the results of this study should be considered against this limitation. In order to ensure triangulation of data to strengthen the integrity of the data multiple cases were selected and data sources varied. Data sources involved data triangulation of audit committee and board minutes, reports to the board and data sources of transcripts of interviews held with the participants. This has ensured that the research was addressed from multiple perspectives (Sekaran & Bougie 2013: 104). Table 1 provides an overview of the three mining companies selected as cases for this study.

Table 1: Overview of mine A, B and C

	Company A	Company B	Company C
Year end	30 June 2013	31 December 2013	31 March 2014
Type of mine	Mid-tier gold	Platinum start-up	Mining services
Sector	Gold	Platinum	Coal and energy
Region of operations in Africa	South Africa	South Africa	South Africa and Sub Saharan Africa
Mining Start up	No	Yes	No
Profit / (loss) for the year in South African Rand (millions)	559	(11)	(576)
Earnings / (loss) per share in South African cents	35	(0.55)	(92)
Listing	AIM / JSE	JSE	JSE

The three mines were selected for their variety of type, sector, and region of operations, lifecycle and profitability to provide a varied picture of mining operation in South Africa. Eleven semi structured interviews were held. These were three participating CACs, two BCs (Company A and C), one NED from

each of the participating companies and the CAE from each of the three companies selected. The semi-structured interviews were based on interview questions (refer to Annexure A) informed by the literature review and were held during the months of October 2014 to May 2015. The full audit committee and board of director meeting minutes were selected for review in each relevant year. Written documents of these meetings were compared with each other to establish whether they corroborated the interviews. Interviews were recorded and independently transcribed. As the data obtained through qualitative analysis involved interview notes, transcripts of interviews, and data analysis and interpretation; this research was focussed on making the correct inferences from the data (Creswell 2009). The data was analysed according to themes and perspectives, by generating categories of information, positioning them in the literature and drawing conclusions (Creswell 2009; Miles & Huberman 1994). Prior to the study ethical clearance was obtained for the research, the participants were made aware of the research and were willing participants in the research. Formal consent was obtained from the participants concerned.

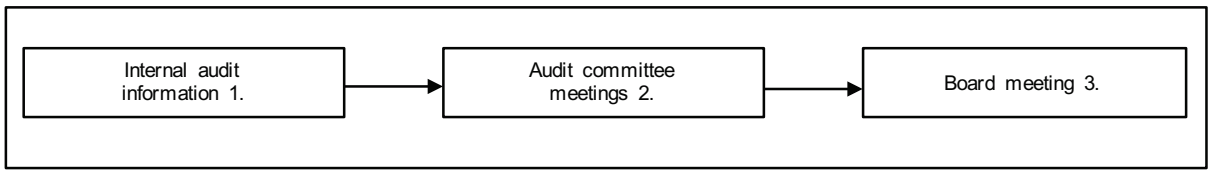
5 PRESENTATION OF FINDINGS

The findings of the study are presented in accordance with the interview questions (refer to Annexure A) which have been informed by the literature review.

What internal audit information is included in the board packs and how is this information communicated to board members? (Interview questions 1 and 2)

The planning of meetings is important (Rogelberg *et al* 2006; Rogelberg *et al* 2007; Volkema & Niederman 1996) and the meetings referred to in the findings were supported by the advanced distribution of agendas and subsequent minutes of the meetings followed. Figure 1 shows the process followed by participants to report internal audit information.

Figure 1: Process followed to report internal audit information



1 *The CAE's were responsible to prepare internal audit information based on the internal audit work performed for a specific period.*
2 *The CAE's presented the internal audit information to the audit committees.*
3 *The CAC's presented the internal audit information to board members. The CAE's did not attend board meetings.*

The CAE's were not present during board meetings (CACs presented the internal audit information to the board) and their views, which follow in the discussions below are based on perceptions from compiling internal audit information and presenting it to the members of the audit committees.

For all participating companies the CAC's were also board members and therefore attended board meetings in that capacity even if they presented internal audit information discussed during audit committee meetings. The other members of the audit committees were also board members. Company A had three board members who were not audit committee members, while for Company B and C there were five and four board members who were not audit committee members respectively.

Earnings restatements and accusations of fraud have undermined public confidence in corporate governance, eliciting discussion on whether communication of internal audit information between audit committees and boards are effective (Paterakis & Cefaratti, 2014; Rezaee *et al* 2003). Questions one and two noted in Annexure A address effective communication with reference to the type of information and the manner in which it is provided. The findings for Company A, B, and C were as follows:

CAC participants
Based on the views shared by CAC participants Company A included internal audit information in audit committee minutes that formed part of the board pack. This was not the case for Company B where no audit committee information, including internal audit information and minutes of the audit committee meeting were submitted in the board pack. Company C distributed the complete audit committee pack, which included the internal audit reports and executive summaries to the board members for information purposes prior to the board meeting. No written summarized audit committee reports were included in the board packs of the three companies. In all instances, only verbal feedback was provided to the board.

BC participants
The BC of Company A concurred that all internal audit reports issued by the internal auditors were included in the board packs. He/she also mentioned that an audit committee summary report including the internal audit information was prepared by the group financial director (FD), approved by the CAC and verbally presented to the board. For Company C the BC participant confirmed that no written audit committee report was included in the board pack and that the minutes of the audit committee meetings were not available. He/she claimed that the board was working six months in arrears with regard to audit committee minutes and relied on the CAC to give verbal feedback to the board. He/she also reported that known critical risks to the business were not communicated to the board and therefore concluded that the risk management was not functional within the Company.

NED participants

NED participants report that for Company A, the CAC verbally presented internal audit information to the board based upon self-prepared notes during the audit committee meeting. For Company B, a short summary of internal audit information obtained by the chairperson during the previous day's audit committee meeting was verbally presented to the board. For Company C the NEDs corroborated that the board pack did not contain any internal audit information. Such information was verbally reported to the board by the CAC.

In order to triangulate the views expressed by the CACs the NEDs and the BC participants of the three selected companies, the minutes of audit committee meetings, and board meetings for the financial year were reviewed. The views of the CAEs were also obtained. Information obtained during the review process is presented in Tables 2, 3 and 4.

Table 2: Internal audit information presented by the CAEs at audit committee meetings

	Company A	Company B	Company C
Meetings	3	4	4
Meeting 1	• Two-year rolling internal audit plan. Areas of review were financial and financial follow up reviews of the previous year. • Plans were not aligned to the risks of the business, as there is no enterprise risk register in operation at the mine.	• The CAE presented no internal status update.	• The 2013 executive summary and detailed internal audit reports over 21 financial processes. • The company has a strategic risk register. Operational risks were not aligned to the internal audit plan.
Meeting 2	• Internal audit engagement letter. The 2013/14 internal audit plan and engagement letter was approved.	• Approved was the half-year internal audit status update and the remaining six months internal audit plan. • The internal auditors developed a financial procedure over a single financial cycle in isolation of the risk register.	• The 2014 internal audit plan and fees presented and approved.
Meeting 3	• Progress against 2013/2014 plan was presented. Progress was on track with the plan. • Internal audit reports on financial process were presented. • Opinions on the adequacy and effectiveness of the systems of internal control were provided.	• Presented and approved was the internal audit status update and the internal audit plan for the remainder of 2013. • No internal audit reviews were performed as agreed in meeting 2.	• No internal audit status update was presented as internal audit work was designed to be performed in the last quarter of the year so that external audit could place possible reliance on the company's systems of financial control.
Meeting 4	• Not meeting held.	• Internal audit status update presented. • Results of internal audits approved in meeting 2 and 3 were discussed. These were two financial cycle reviews.	• The strategic enterprise risk management report was presented. • The 2014 internal audit plan progress update was presented.
Communi-cation style	• The written internal audit plans, progress reports and detailed internal audit reports were clear and concise. • The CAE.to members of the audit committee provided a detailed verbal feedback.	• The written internal audit plans, progress reports and detailed internal audit reports were clear and concise. • The CAE.to members of the audit committee provided a detailed verbal feedback.	• The written internal audit plans, progress reports and detailed internal audit reports were clear and concise. • The CAE provided a detailed verbal feedback to members of the audit committee.
Timing of meeting	• One day before the board meeting.	• One day before the board meeting.	• One week before board meeting.

CAE participants

The CAE for all three companies concurred with the internal audit information presented at audit committees in Table 2. Company A's CAE advised that pre-meetings are held with the CACs which strengthens his/her understanding and conclusions of the information. As Company B was a start-up mine, the focus of internal audit was to develop financial procedures. The CAE of Company B reported the internal audit plan was developed via "*consultation based work where we had developed policies and procedures for them*" to assist management in policy and procedure development and subsequently provide assurance services. A concern raised by the CAE was that their executive summaries were translated into foreign languages and concern was raised on inadvertent misrepresentation of information to the main shareholder as no feedback verification loop was provided. Company C's CAE had no pre-meetings with the CAC and verbally presented their executive summary at the audit committee meeting.

Internal audit information for all companies included financial reviews that were planned, executed and clearly presented by the CAE's within required timelines at the audit committee meetings. An opinion on the adequacy and effectiveness of the systems of internal control was provided in reports and verbally presented. For Company A and C the internal audit plans were not aligned to the risks of the business and operational reviews were not planned and executed.

Table 3: Internal audit information from minutes of audit committee meetings

	Company A	Company B	Company C
Number of meetings	3	4	4
Meeting 1	• No opinion provided on the adequacy and effectiveness of the systems of internal control. • The internal audit plans were debated, but not aligned to the risks of the business.	• Internal auditors requested to work closely with risk management.	• Detailed internal audit information was not aligned to the company risk register. • Processes discussed were information technology, general controls, disaster recovery plans, stock, procurement and asset management reviews.
Meeting 2	• The previous internal audit reports were debated. • Previous internal audit action plans were debated. • Operational internal audit plans were not discussed.	• Internal audit plan, fees and combined assurance plans were discussed and approved.	• Internal audit plans and fees were approved.
Meeting 3	• Internal audit was required to give an opinion on the adequacy and effectiveness of the systems of internal control. • Critical financial internal control weaknesses were presented and debated.	• Revised internal audit plans were discussed and approved.	• The audit committee minutes were not available in the minute book. They could not be found.
Meeting 4	• No meeting held.	• Feedback provided by internal auditors was debated.	• The internal audit plan was not discussed but taken "as read". • Challenges regarding operational risk were noted.
Style of communication	• Written audit committee minutes were cryptic and unstructured. • Verbal feedback was provided to the board by the CAC.	• The CAC did not prepare a written report to the board. • Verbal feedback provided to the board by the chairperson or surrogate.	• The CAC did not prepare a written report to the board. • Verbal feedback provided to the board by the CAC.
Timing of meeting	• One day before the board meeting.	• One day before the board meeting.	• One week before board meeting.

Table 4: Internal audit information from minutes of board meetings

	Company A	Company B	Company C
Number of meetings	5 but only 3 related to the audit committee meetings.	4	4
Meeting 1	• There was no formal feedback on internal audit information. Minutes state, "The feedback was taken as read".	• Internal audit information reported did not corroborate with the audit committee meeting minutes.	• Internal audit information per Table 3 (meeting 1) was not included in the board minutes.
Meeting 2	• No discussion on internal audit information though there was extensive debate at the audit committee meeting (refer to Table 3 meeting 2).	• No discussion of internal audit information (refer to Table 3, meeting 2). • Minutes stated "board committee considered and noted various reports" but these were not specified.	• Internal audit information per Table 3 (meeting 2) was not included in the board minutes.
Meeting 3	• Critical financial internal control breakdowns discussed at the audit committee meeting was not discussed at the board meeting (refer to Table 3, meeting 3).	• Internal audit plan was approved.	• No discussion of internal audit information (refer to Table 3, meeting 3).
Meeting 4	• Not applicable.	• Internal audit plan for the fourth coming year was approved.	• The internal audit plan was communicated. • Challenges regarding operation risk were not mentioned.
Meeting 5	• Not applicable.	• Not applicable.	• Not applicable.
Style of communication.	• Chairperson of audit committee gave verbal feedback. No written feedback report prepared.	• Chairperson of audit committee gave verbal feedback. • In some instances, this was delegated to a surrogate who had no experience of internal audit.	• The chairperson of audit committee gave verbal feedback and presented a written report. However, these written reports could not be obtained.

For all companies fragmented internal audit information was included in the audit committee minutes and based on the minutes internal audit reports and plans were debated. It was however confirmed that these were not aligned with the companies risk registers. No operational internal audits were performed. The CACs did not prepare a written report and gave a verbal feedback to the board.

Based on a summary of the board minutes (refer to Table 4), it appears that internal audit information was not discussed and board members relied on the verbal feedback provided by the CAC. The minutes did not report whether the board members debated the verbally reported internal audit information.

Summary

Internal audit information included in board packs varied and ranged from the inclusion of internal audit reports with supported summaries to a disregard of internal audit information. For Company A and B no written report on internal audit information to the board was included in board packs and only verbal feedback was presented by the CACs. For Company B a surrogate to the chairperson was used to present audit committee information and he/she had no experience in internal audit which could lead to information loss. The reasons mentioned for verbal presentations are that board meetings are held the day after the audit committee meeting and there was no time to prepare a written report. Information noted in audit committee meeting minutes did not corroborate to that recorded in board minutes further corroborating weak upward internal audit information dissemination to the board. Such the effectiveness of internal audit information communicated between the audit committee and the board of directors is questionable.

What are the strengths and weaknesses of the information and how does the board act upon it? (Interview questions 3 and 4)

Stakeholders require boards of directors to be well informed on important risk areas and matters relating to the strategic objectives of their companies. This information is obtained through effective communication from a well-functioning audit committee (IoD 2009; Davies 2008; Cohen *et al* 2007; Mallin, 2003). The key to management communication is to elicit action (Robbins & Judge 2013; Siegel & Schultz 2011) and therefore strengths and weaknesses of internal audit information and how the board acts upon it are important questions to ask (Paterakis & Cefaratti 2014). Adler (2012:15) maintains a strength of the content of the communicated information represents a shared strategic goal.

CAC participants

The CAC at Company A perceived awareness that the IAF reviewed the accounting processes of the company as a strength of internal audit information. It provided assurance on the adequacy and effectiveness of the financial controls of the company, consequently the board partially relied on internal audit information. An information weakness identified by the CAC was that internal audit plans were not based upon formal risk assessments as the internal audit work plan was compiled from discussions with the executive management and the chair of the audit committee. The CAC further asserted, "*the internal audit information did not address the adequacy and effectiveness of operational controls of the company and mining operations and risk registers were not considered in the internal audit work plan*". This resulted in significant risks not being communicated to the board. The CAC believed that although internal audit information was verbally communicated, it was accurate and complete as it was obtained the previous day (the board meeting was followed by the audit committee meeting). He/she however acknowledged that this information was verbally presented, that errors of interpretation, accuracy and specifics may occur which could compromise the accuracy validity and completeness of the reported information. The verbal presentation to the board was not validated to the minutes of the audit committee meeting. At Company C, the complete audit committee pack that includes the internal audit information was presented to the board. The CAC expressed some reservations because there was a lack of understanding of risk management, on how to inculcate it into the business and how to link it to the internal audit work plan which he/she ascribed to management and the board not understanding risk. He/she then confirmed that the board was uncertain that all risks from the mine were communicated to the audit committee and the board. Another weakness identified by the CAC was that communication and issues discussed and considered at the audit committee were repeated at board meetings, resulting in a repetition of what was previously discussed. He/she however maintained that this practice afforded the board with a good understanding of the internal audit findings and recommendations arising from the audit committee meetings.

BC participants

The BC at Company A perceived that information presented by the CAC was debated and understood although these were not minuted, (refer to Table 4). As the CAC was perceived to be competent and experienced, the quality of the information was not questioned. However, the information did not identify significant *top ten* risks that could harm the business financially and damage its reputation. The BC attributed this to the possibility that the internal auditor does not communicate significant findings to the audit committee and thus to the board. A mitigating factor according to the BC of Company A was that the majority of board members sat in audit committee meetings and consequently, all recommendations for improvement in the systems of internal control provided by the internal auditors were indirectly communicated to board members. The BC at Company C reported that only internal audit financial information was reported to the board. The BC at Company C mentioned that "*the banks were on our back, they were saying, covenants were being broken, are we going to survive?*" The internal audit information was not deemed valuable as the board was more concerned about financial sustainability. Due to significant stock write offs the company almost went out of business. The BC at Company C perceived the IAF to be used by the company as a

tick box, as *form over substance*. Consequently, the risks identified by the IAF were not critical to the business. Furthermore, the function did not report on operational information and as management had not implemented an effective risk management process the IAF could not align its work coverage plan to high-risk areas of the business.

NED participants

The NED of Company A perceived the strength of internal audit information lay in its independence and the CAE's verbal presentation to the audit committee. Issues are debated (not minuted as such, refer to Table 4) at a board level and where serious acted upon. A further strength is that all three NEDs preside on both board and audit committee meetings. Weaknesses according to the NEDs relate to lack of discussion on technical information, no pre-committee involvement and no feedback from the board to the audit committee. Company B was a start-up so there was a vacuum in the systems of internal control that the internal audit information addressed through the development of policy and procedures. The integrity and the quality of the internal audit information was not questioned and according to the NED, the board debated and acted on issues. (These debates are not reflected in the minutes. Refer Table 4). A weakness according to the NED participant at Company B was that the internal auditors did not adhere to their internal audit plan due to policy and procedure development. He/she reported that the internal audit reviews agreed in their second meeting were not completed by meeting three. The NED participant at Company C could not adequately address the question, which indicated limited access or under-standing of internal audit information and risk though he/he conceded that debate of these issues at both committee meetings assisted in the understanding of company risk. (Also not reflected in the minutes. Refer Table 4).

CAE participants

CAEs of participating companies did not attend board meetings and therefore their views are based on information presented to audit committees and attendance at these meetings. The CAE of Company A believed pre-audit committee meetings greatly assisted in the understanding and communication of internal audit information to executive management and the CAC. Audit committee meetings were short however, providing limited opportunity for debate. NEDs did not debate issues at the audit committee meetings. The CAE was concerned about the lack of effective reporting on enterprise risk management and the inability to develop internal audit plans aligned to the significant risks of the business. According to the CAE of Company B, internal audit information provided assistance in the development of systems of internal control. This assisted the company to value internal audit. A weakness noted by the CAE of Company B was the inability of the company to implement an effective enterprise wide risk management system. Significant mine risks known by the internal auditors were not reflected on the company risk register and were not aligned to the internal audit plan. The CAE participant of Company C perceived the volume and timing of internal audit information to be a weakness because high demands are placed on the audit committee and board to consume it. For example, twenty one (21) financial processes were audited during the last quarter and reported in the first meeting of the following year. The CAE was concerned about the audit committee's ability to digest the information as borne out by the lack of questions raised in the first meeting and expressed doubt about its effective reporting to the board.

Summary

Although the board minutes of the three participating companies did not refer to debates on internal audit information, BCs and NEDs presented contrasting views. They asserted that board members debated such information. The fact that the internal audit information elicited actions from executive management could be regarded as a strength and agrees with the literature (Robbins & Judge 2013:573). However, two BC participants mentioned only partially reliance on the IAF due to limited operational process coverage. Internal audit plans were also not aligned to risks of the company and a recurring theme was the concern that significant operational risks were not communicated to the audit committee or board. It therefore appears as if strategic goal achievement was not emphasized in internal audit information and this could represent a weakness. For all companies, internal audit information was verbally communicated to the board. This was because the board generally met soon after the audit committee and there was no time to prepare a written report. Some concern was expressed that there could be errors of interpretation and accuracy in verbal presentations. Importantly, verbal presentations were inaccurate as information reported at Company B's audit committee meetings was incorrectly recorded in board minutes and did not agree with participants views that internal audit information was debated. The verbal presentation of such information therefore appears to be a weakness. For Company C, most communication discussed at audit committee meetings was repeated at board meetings and although the CAC expressed concern about such practice he/she acknowledged that the information produced was well understood by board members and acted upon. Company C's board was more concerned about sustainability, and significant asset write offs than internal audit information. It appears that communicating internal audit information was not a shared strategic goal (Adler 2012:15) and therefore carried less weight. This could also be regarded as a weakness. Table 5 summaries the findings of the strengths and weaknesses of the internal audit information presented to the board.

The fact that nearly all members of the participating companies' boards also sat on the audit committees and considered internal audit reports during audit committee meetings, could be regarded as a mitigating measure. CAEs were not invited to attend board meetings. The IAF was used as a *tick box* rather than, substance over form.

Table 5: Summary of the strengths and weaknesses of the internal audit information presented to the board

Strengths	Weaknesses
• The board acted on internal audit information presented.	• Internal audit information was not aligned with the risks of the business and industry. • Internal audit information was not considered a strategic goal – other matters were considered more significant. • Internal audit information as presented verbally could result in inaccuracies and omissions.

What do you consider the strengths, weaknesses and barriers in the communication process? (Interview questions 5 and 6)

Previous internal audit studies have emphasized the benefits of effective communication (Paterakis & Cefaratti 2014; Drent 2002). However, the literature offers little insight into operational situations surrounding audit committee interaction with the board. Effective communication indicators include rapport, sharing, listening, clarifying and trust built by congruency with words and action (Adler 2012; Colquitt *et al* 2007).

CAC participants

The CAC at Company A reported that in addition to the formal audit committee meetings, informal meetings were held between the CAC, the executive, external auditors and internal auditors. This practice was established because the previous chief executive officer (CEO) did not communicate effectively at board meetings. The communication was not open and transparent and was held in side sessions with individuals. The CAC mentioned lack of trust in the process as the previous CEO *"loved to play divide and rule"* The CAC at Company B reported that dominant board members stifled the flow of communication. Slow board resolutions took a lot of time because decisions were taken offshore. Another barrier identified was that some members of the audit committee and board did not speak English and they required translation services. The technical strengths of the translator were unknown by the members. Consequently, debate was slow, boring, and interruptions were frequent causing internal audit information to be lost in translation. The CAC of Company B believed that foreign hierarchical cultural barriers negatively affected the debate ("lack of debate") and level of trust in the debate between members. The CAC at Company C perceived the financial executive members of the Company were "not audit friendly". He/she perceived the chief financial officer (CFO) to be dominant, someone who switched auditors often and had a culture of blaming the auditors for weak systems of internal control. The CAC of company C stated that the CFO regarded *"each and every audit finding as a direct reflection on his ability".* Members of the executive took audit findings personally. He/she maintained that the culture at the audit committee was not transparent to discuss and resolve issues and this was exacerbated by disharmony in the relationships between the executive, a weak BC who could not resolve conflict with executive management and that the executive perceived there were more important issues to discuss than internal audit information. He/she supported the statement by claiming the risks facing the business were not communicated to the audit committee and consequently there was no debate around the risks facing the company. The internal auditors were required to assist the executive with a risk management report the day before the audit committee. He/she further believed there was a lack of informal interaction between the chair of the audit committee and the internal auditors.

BC participants

At Company A all board members but one NED were members of the audit committee and this practice promoted effective communication between the audit committee members and the board of directors. The audit committee meetings took place the day before the board meeting. There was no time for the CAC to write a formal audit committee report to the board of directors. When this occurred, a verbal presentation was presented. Consequently, the BC expressed concern that internal audit information was omitted or misconstrued. A mitigating factor is that nearly all board members also serve on the audit committee and were present when the CAE presented the internal audit information. The CAC however had delegated the writing of the audit committee report to the group FD. The BC perceived that some business issues were covered up and not reported to the board and stated *"if something goes wrong, that it is conceivable that it might be covered up".* He/she ascribed it to a lack of trust and fear that there would be negative consequences when the executives made errors. The BC mentioned that most of the board communication took place in informal settings outside of formal board meetings. For Company C the BC acknowledged that the board was dysfunctional and led to a practice of non-communication. He/she acknowledged that the FD "*wouldn't accept responsibility"* and we "*had a breakdown between the board, the audit committee and the executive".* The FD did not take responsibility for adequate and effective systems of internal control and the board was only made aware of significant losses after they had occurred. Due to a lack of supervision, this information was not timeously communicated. At the time, the IAF was restricted from reviewing known significant risks to the business and consequently risk management was not functional. The BC participant believed internal audit was a *tick box affair*. The audit committee spent much time discussing external audit matters and did not pay attention to internal audit information. The internal audit plan was financially orientated and driven by the FD. Reporting on operational information did not occur. The BC participant acknowledged that board members did not understand technical issues of the company and therefore some board members were not committed to the strategy of the company. The BC mentioned in

some instances board communication channels were by-passed and they had out of board meetings by e-mail. He/she reported that members arriving late at board meetings which caused meeting interruption. The BC mentioned that he/she could not enter into and control a strategic debate due to dysfunctional relationships at the executive. Members of the executive acted *"without trust and argued at board meetings"*. He /she further believed that board members did not understand the company strategy and their roles and responsibilities in the company. This led to verbal and written disagreements break down in relationships and ineffective communication.

NED participants

The NED participants at Company A were concerned that internal audit information was not regularly, throughout the year communicated and recommended regular reporting of findings would enhance communication. The NED of Company, A stated *"I think our worst thing, all of us, is time"* and *"not enough time is given to debate".* There was lack of time provided to debate findings. The NED at Company B advised that communication was open and enough time was given to discussions however, effective communication was severely slowed down due to foreign speaking members and recommended an English speaking FD who understood the South African legal and financial system. The NED of Company C was concerned that the audit committee minutes were not included in the board pack but that this was offset by adequate verbal communication. He/she did not perceive any barriers to the communication process.

CAE participants

CAEs of participating companies did not attend board meetings and their views relate to audit committee meetings. The CAE of Company A reported that the communication between him/her and the audit committee was mainly on an informal basis, which is a strength and weakness. A strength as communication takes place but a weakness as no mechanism is in place to ensure up and downward communication takes place between the audit committee and board. There is no loopback mechanism. Concern was raised that communication by the CAC to the board was verbal and there was potential for information loss from pre-audit committee meetings, to the audit committee to the board meeting. The CAE of Company B considered the audit committee communication process significantly weak due to foreign translation, culture, in-committee side meetings, and a lack of trust manifested as lack of transparency and infighting between South African and foreign members. The CAE of Company C considered formalized communication practices as a strength. Weaknesses noted were a dominant FD, limitation on internal audit scope, non-alignment of the internal audit plan to company risks and strategic objectives, weak risk management practices and a weak relationship with the CAC.

Summary

The communication process between the audit committee and the board is influenced by board dynamics. For example, ineffective communication of a previous CEO at Company A lead to a communication protocol driven by informal (one-on-one meetings) rather than formal meetings. With reference to past practices, various weaknesses in the former communication process were identified; not being open, transparent thus compromising trust building. The fact that communication by the CAC was verbal could result in internal audit information being omitted or misconstrued. This could be mitigated if the majority of board members sit on the audit committee as in the case of the participating companies. The final audit committee report was delegated to the group FD further risking loss of information. Company B had a weak communication process, which could be ascribed to cultural, and language barriers. There were dominant board members, slow board resolutions, members who did not understand English, the use of translation services, slow debate, interruptions, and a lack of trust in debate due to hierarchical cultural barriers. Consequently, most of the board communication took place outside formal board meetings, a strength that at least matters were communicated but also a weakness because the process was not open and transparent. Company C exhibited severe weakness in the communication process due to disharmony in relationships between the executive and a lack of trust. It exhibited the following dysfunctional communication barriers: pre-conceived perceptions that some executives were not audit friendly, a dominant FD who had a culture of blame and not taking responsibility and members of the executive who were overly sensitive towards internal audit findings. There were personal conflicts between the executives. Together these have resulted in a culture not to discuss and resolve issues. An interesting finding is that the CACs and BCs were quite outspoken about weaknesses and barriers in the communication process of all participating companies, while the NEDs had contrasting views and did not discuss board differences. The NEDs of company C for example did not perceive any barriers in the communication process. The BC of Company C however expressed some reservations on the understanding of board members of the knowledge of business and the company strategy. It could be questioned whether clear messages were sent which as Adler (2012:45-56) suggest should clarify assumptions. This is another weakness in the communication process. Table 6 summarizes the strengths, weaknesses and barriers of the communication process.

How do you debate controversial issues on breakdowns in the systems of internal control? (Interview question 7)

Management of controversial debate in board and audit committee is important to drive management action and effective communication elicits action (Robbins & Judge 2013; Siegel & Schultz 2011). Debating controversial issues effectively will build rapport, assist in the sharing of strategic goals, and ensure active listening which assists in clarifying debate (Adler 2012; Hubbard 2000).

Table 6: Summary of the strengths, weaknesses and barriers of the communication process

Strengths	Weaknesses	Barriers
• Informal sessions were held to discuss internal audit information.	• Instances were referred to where the communication process could not be considered effective because it did not make provision for: ○ open debates, ○ to be transparent, ○ to build trust, ○ clear messages to be portrayed. • The frequency of communicating internal audit information.	• Culture barriers. • Language. • Board dynamics: ○ dominance of a single board member, ○ disharmony in relationships of board members. • Preconceived perceptions about internal audit. • Conduct of board members: ○ Arriving late, ○ Interrupting debates, ○ Displaying limited understanding of internal audit matters.

CAC participants

Based on views expressed by the CAC at Company A, there was robust debate during audit committee meetings relating to weaknesses in systems of internal control. This enabled the audit committee to resolve issues and to report to the board. The CAC at Company B shared this sentiment and followed the same process. The CAC at Company C reported that controversial issues and breakdowns in the systems of internal control were debated and resolved during informal meetings. These meetings were held outside of the formal meetings of the audit committee and board. He/she acknowledged the need for greater informal interaction between the CAC and the internal auditors.

BC participants

The BC at Company A expressed favorable views. He/she reported that the CAC verbally presented the audit committee report after the controversial issues had been debated during the audit committee meeting. A strong CAC and FD further debated all issues related to systems of internal control during board meetings. From views expressed by the BC at Company C, debate during board meetings was poor particularly between the FD and board. He/she ascribed it to the fact the FD took matters personally and refused to accept the responsibility to correct weaknesses in the systems of internal control.

NED participants

NEDs of Company A and C concurred that controversial issues were debated and discussed effectively during the audit committee meetings. Where necessary management were excused to allow the CAEs to discuss points of contention freely. The NED of Company B reported that although time was allowed to debate any controversial issues during board meetings due to cultural, language differences and a dominant foreign shareholder these debates were not constructive.

CAE participants

CAEs did not attend board meetings and only reflected on audit committee meetings. The CAE of Company A expressed generally favorable views. In-committee debates were rare as controversial issues were debated and resolved through the CAC's involvement in meetings held prior to formal audit committee meetings. Debates in Company B were perceived as dysfunctional and were confrontational, as foreign audit committee and board members did not recognize internal audit findings as beneficial. The CAE ascribed it to cultural differences. The CAE of Company C confirmed that debate was poor between the FD and members of the audit committee and that there was tension between the executive, the CEO and the FD. The FD interrupted debates and the CAE mentioned that *"because of this aggressive behavior from individuals. Specifically the FD, it was as if the chair then just to avoid conflict rather would back off and then say okay well just prepare and come prepared next time"* the FD withheld information from the audit committee.

Summary

For all three companies an attempt was made to debate controversial issues. It appears that controversial issues on breakdowns in systems of internal control was mainly conducted at audit committee meetings during which the CAEs were present. Board dynamics, as previously reported again influenced the debate at Company B resulting in ineffective communication.

What is your perception of the interaction of the chairperson of the audit committee and members of the board and what attributes are needed? (Interview questions 8)

The key to management communication is to elicit action. This involves upward, downward and lateral communication (Robbins & Judge 2013; Siegel & Schultz 2011) during which CACs should have the necessary attributes to incalcate at the beginning of a meeting or process goals identification (Locke & Latham 2006).

CAC participants

The CAC at Company A believed that he/she could be regard as assertive and he/she was well respected by the board, especially by the FD and CEO. He/she identified the following important attributes: courage in communication, taking responsibility when there were company challenges, assertive, knowledgeable and being a coach to the audit committee or board of directors. CACs at Company B and C held similar views and added knowledge and skill of the subject matter, discipline, eloquence, being audible, un-emotional, displaying emotional intelligence particularly around sensitivities of culture and dealing with the issue and not the person were identified as needed attributes.

BC participants
The BC at Company A regarded the CAC as diligent and well prepared for meetings and able to debate issues with members of the board. He/she valued the following attributes: being knowledgeable, assertive and displaying strong leadership skills. The CAC should have a sound financial and operating knowledge of the business, and understand the mining industry. This will ensure effective communication. The BC at Company C expressed concern about the information tabled by the CAC, which in some instances was not understood by board members. He/she maintained that the CAC should not be domineering, and should participate in issues discussed. The chairperson should be the *conductor of the audit committee or board* and come across unnoticed, yet effectively communicate the issues raised by the members. The CAC should display empathy and understand his fellow member's personality and capabilities. The chairperson should be strategy and goals orientated, a coach and summarize long debates. Most importantly, the CAC should ensure proper minute taking is performed, as this is the only record of conversation the board has.

NED participants
The NED of company A regarded the CAC as a *strong, experienced and respected individual* who displayed courage to confront difficult issues. The NED of Company B perceived interaction between the CAC and board members to be *short yet precise* and for the NED as company C it was satisfactory. The NEDs of all companies recognized the CAC attributes of an ability to listen, technical knowledge, experience written, verbal and articulation skills, assertiveness and the ability to lead a strategic debate.

CAE participants
The CAE's of the three companies had similar views to the non-executive directors

Summary
Views expressed about the interaction of the CACs with board members mirrored participants perceptions about the effectiveness of communication. Where the latter was positive, the interaction was also perceived in a positive light. Although Company B and C had weak communication, participants of the three companies recognized the attributes needed by the CAC for effective communication. All agreed that knowledge of the subject matter, being assertive, courageous, taking responsibility, and displaying empathy are necessary. Being the conductor of the meeting, and instilling a strategic outcome debate was also deemed important. The effective minute takings of conversations were necessary.

6 CONCLUSIONS, RECOMMENDATIONS AND AREAS FOR FUTURE RESEARCH

This article examines audit committee's communication on internal audit to boards of directors, a topic that has come to the fore due to recent local and international corporate failures. Previous studies raised concern over effective audit committee communication, a relatively unexplored area. There is anecdotal evidence that internal audit information may be omitted, diluted or misrepresented to the board due to a variety of reasons and it forms the focus of this article. It adds to the current knowledge as the literature review revealed that most audit committee studies focus mainly on audit committee composition, its authority, resources and diligence and not on the actual process of communication (DeZoort *et al* 2002). The study had certain limitations. The research was limited to three listed companies on the JSE that were operating in the mining sector (chosen due to recent mining sector strikes that have affected the South African economy) which offered triangulation opportunities. The literature offers little insight into the operational situations surrounding audit committee communication and the manner of non-verbal, written, oral or interpersonal interaction between these committees and whether such communication was effective. Consequently; communication literature was drawn upon to determine effective communication indicators. Semi structured interviews were held to determine communication effectiveness with participating CACs, BCs, NEDs and CAEs and eight interview questions informed by the literature review were answered.

The findings of the study revealed that limited internal audit information was included in board packs and this information was poorly communicated. This weakness was mitigated as most board members participated in audit committee meeting. Information communicated did not always corroborate with the contents of the internal audit reports presented by the CAEs at the audit committee. Internal audit information reported in the minutes of board and audit committee minutes did not always agree. The CACs did not prepare a written report and only verbal feedback was provided to the board. The findings show that internal audit information presented to the board was limited to a review of the financial process and was not aligned with company risks. Significant operational risks were not communicated to the audit committee or the board and it therefore appears that strategic company goals were therefore not emphasized in the internal audit information. These could be considered as weaknesses while the strength of the information reported on was that it elicited board action.

The findings show that the communication processes had strengths, weaknesses and barriers were identified. A strength was that internal audit information was discussed, also in informal meetings other than audit committee and board meetings. Weaknesses identified were the lack of an open, transparent debate, which could build trust between members. Infrequent reporting of internal audit information was deemed as a further weakness. In some instances board dynamics such as established practices based on the past, conduct of dominant board members, and disharmony in relationships of board members acted as barriers. Culture and language barriers also resulted in ineffective communication processes. The conduct of members (arriving late for meetings, interrupting debates, and poor understanding) could also be regarded as barriers. Controversial issues on breakdowns in the systems of internal control were debated at all three participating companies but these were mainly held during audit committee meetings. Participants at all

three of these companies recognized the attributes needed by a CAC for effective communication. These include having knowledge of the subject matter, being assertive, courageous, taking responsibility, and displaying empathy where necessary. Being the conductor of the meeting, and instilling a strategic outcome debate was important. The study found perceptions about the interactions of CACs with board members mirrored their views about the effectiveness of the communication process.

As this article was limited to three mining companies future research should explore a larger sample of companies, to determine whether the results from this study are endemic to the South African business community. Such research could focus on the required communication protocols to ensure useful, accurate and complete internal audit information is presented to the board of directors. Future studies should be undertaken to determine the control mechanisms necessary to ensure board pack information is complete. CAC communication practices need to be explored to decide whether communication conventions should be formalised. Attributes of effective communication between the CAC and board could be studied to determine whether they predict effective strategy implementation.

REFERENCES

Abbott, L.J. & Parker, S. 2000. Auditor selection and audit committee characteristics. *Auditing: A Journal of Practice & Theory*, 19(2):47-66.

Abbott, L.J., Parker, S. & Peters, G. F. 2004. Audit committee characteristics and restatements. Auditing: A Journal of Practice & Theory, 19(2):47-66.

Abbott, L.J., Park, Y. & Parker, S. 2000. The effects of audit committee activity and independence on corporate fraud. *Managerial Finance*, 26:55-67.

Abdolmohammadi, M.J. & Levy, E.S. 1992. Audit committee members' perceptions of their responsibility. *Internal Auditing*, Summer:53-63.

Abdolmohammadi, M.J., Ramamoorti, S. & Sarens, G. 2013. *CAE strategic relationships. Building rapport with the executive suite.* Altamonte Springs: The Institute of Internal Auditors Research Foundation (IIARF).

Adams, M.B. 1994. Agency theory and the internal audit. *Managerial Auditing Journal*, 9(8):8-12.

Adler, G. 2012. *Financial times briefings: Management communication.* (1st ed.) Edinburgh Gate: Prentice Hall.

Aldamen, H., Duncan, K., Kelly, S., McNamara, R. & Nagel, S. 2012. Audit committee characteristics and firm performance during the global financial crisis. *Accounting and Finance*, 52:971-1000.

Archambeault, D. & DeZoort, F.T. 2001. Auditor opinion shopping and the audit committee: An analysis of suspicious auditor switches. *International Journal of Auditing*, March:33-52.

Avison, L. & Cowton, C.J. 2012. UK audit committees and the revised Code. *Corporate Governance*, 12(1):42-53.

Bang, H., Fuglesang, S.L. Ovesen, M.R. & Eilertsen, D.E. 2010. Effectiveness in top management group meetings: The role of goal clarity, focussed communication, and learning behavior. *Scandinavian Journal of Psychology*, 51:253-261.

Barua, A., Rama, D.V. & Sharma, V. 2010. Audit committee characteristics and investment in internal auditing. *Journal of Accounting Public Policy*, 29:503-513.

Beasley, M.S., Carcello, J.V., Hermanson, D.R. & Lapides, P. D. 2000. Fraudulent financial reporting: consideration of industry traits and corporate governance mechanisms. *Accounting Horizons*, 14:441-454.

Beasley, M.S. & Salterio, S. 2001. The relationship between board characteristics and voluntary improvements in audit committee composition and experience. *Contemporary Accounting Research*, Winter:539-570.

Bisseker, C. 2014. Economy: waters still troubled. *Financial Mail*, 11 December. [Online]. http://www.financialmail.co.za/features/2014/12/11/economy-waters-still-troubled [Accessed: 2 October 2016].

Braiotta Jr. L., Gazzaway, R.T., Colson, R. & Ramamoorti, S. 2010. The audit committee's report and concluding observations. *The Audit Committee Handbook.* Hoboken: John Wiley Inc:346-362.

Carcello, J.V., Hermanson, D.R. & Neal, T.L. 2002. Disclosures in audit committee charters and reports. *Accounting Horizons*, 16:291-304.

Charan, R. 2005. Information architecture. In: *Boards that deliver. Advancing corporate governance from compliance to competetive advantage.* San Francisco: Jossey-Bass:59-60.

Clarke, T. 2004. Cycles of crisis and regulation: The enduring agency and stewardship problems of corporate governance. *Corporate Governance: An International Review*, 12(2):153-161.

Coetzee, P. & Fourie, H. 2009. Perceptions on the role of the internal audit function in respect of risk. *African Journal of Business Management*, 3(13):959-968.

Cohen, J., Gaynor, L.M., Krishnamoorthy, G. & Wright, A.M. 2007. Auditor communications with the audit committee and the board of directors: Policy recommendations for future research. *Accounting Horizons*, 21(2):165-187.

Cohen, J., Krishnamoorthy, G. & Wright, A. 2002. Corporate governance and the audit process. *Contemporary Accounting Research*, Winter:573-594.

Cohen, J.R. & Hanno, D.M. 2000. Auditors' consideration of corporate governance and management control philisophy in preplanning and planning judgements. *A Journal of Practice and Theory*, 19:133-146.

Collier, P. & Gregory, A. 1999. Audit committee activity and agency costs. *Journal of Accounting & Public Policy*, 18:311-332.

Colquitt, J., Scott, B.A. & LePine, J.A. 2007. Trust, trustworthiness, and trust propensity: a meta- analytic test of their unique relationships with risk taking and job performance. *Journal of Applied Psychology*, 92(4):909-927.

Creswell, J.W. 2009. *Research design: Qualitative, quantitative and mixed method approaches.* Los Angeles: SAGE.

Davies, M. 2008. *Effective working relationships between audit committees and internal audit - the cornerstone of corporate governance in local communities, a Welsh perspective.* Pontypridd: Springer.

DeZoort, F.T. 1997. An investigation of audit committees' oversight responsibilities. *Abacus*, 33:208-227.

DeZoort, F.T., Hermanson, D. & Houston, R.W. 2003. Audit committee support for auditors: the effects of materiality justification and accounting precision. *Journal of Accounting and Public Policy*, 22(3):175-199.

DeZoort, F.T., Hermanson, D.R., Archambeault, D.S. & Reed, S.A. 2002. Audit committee effectiveness: A synthesis of the empirical audit committee literature. *Journal of Accounting Literature*, 21:38-75.

Drent, S. 2002. The quest for increased relevance. *Internal Auditor*, 59(1):49-55.

Eulerich, M., Theis, J., Velte, P. & Stigtbauer, M., 2013. Self-perception of the internal audit function within the corporate governance system - empirical evidence from the European Union. *Problems and Perspectives in Management*, 11(2):57-72.

Fama, E. & Jensen, M. 1983. Seperation of ownership and control. *Journal of Law and Economics*, June:301-325.

Financial Crisis Inquiry Commision, 2011. *The financial crisis inquiry report.* Final report of the National Commission on the causes of the financial and economic crisis in the USA. Washington:FCIC.

Goodwin-Stewart, J. & Kent, P. 2006. The use of internal audit by Australian companies. *Managerial Auditing Journal*, 21(1):81-101.

Hirsch, A. 2005. *Season of hope. economic reform under Mandela and Mbeki.* (1st ed.) Pietermaritzburg: UKZN Press and IDRC.

Holland, T.P. 2002. Board accountability: Lessons from the field. *Non Profit Management & Leadership,* 12(4):409-428.

Hubbard, L.D. 2000. Talk first, write later. *Internal Auditor*, 57(6):22.

Institute of Internal Auditors (IIA). 2011. *International standards for the professional practice of internal auditing.* South African Student Edition ed. Johannesburg: IIA.

Institute of Directors (IoDSA). 1994. *King report on corporate governance for South Africa.* Johannesburg: IoDSA.

Institute of Directors (IoDSA). 2002. *King report on corporate governance for South Africa.* Johannesburg: IoDSA.

Institute of Directors (IoDSA). 2009. *King report on corporate governance for South Africa.* Johannesburg: IoDSA.

Institute of Directors (IoDSA), 2016. *Draft King IV report on corporate governance for South Africa 2016.* Johannesburg: IoDSA.

Jensen, M. & Meckling, W. 1976. Theory of the firm: managerial behavior, agency costs, and ownership structure. *Journal of Financial Economies*, 3:305-360.

Kalbers, L.P. 1992(a). An examination of the relationship between audit committees and external auditors. *The Ohio CPA Journal*, 51(6):19-27.

Kalbers, L.P. 1992(b). Audit committees and internal auditors. *Internal Auditor*, December:37-44.

Kalbers, L.P. & Fogarty, T.J. 1993. Audit committee effectiveness: An empirical investigation of the contribution of power. *Auditing: A Journal of Practice & Theory*, 12(Spring):24-29.

King, M.E. 2006. The audit committee. In: *The corporate citizen. Governance for all entities.* Johannesburg: Penguin.

King, M.E. 2010. The synergies and interaction between King III and the Companies Act 61 of 2008. *Acta Juridica*, 446-455.

Kirkpatrick, G. 2009. The corporate governance lessons from the financial crisis. *OECD Journal: Financial Market Trends*, 3(1):61-67.

Klein, A. 2002. Econonic determinants of audit committee independence. *The Accounting Review*, *77*:435-452.

Lary, A.M. & Taylor, D.W. 2012. Governance characteristics and role effectiveness of audit committees. *Managerial Auditing Journal*, 27(4):336-354.

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

Locke, E.A. & Latham, G.P. 2006. New directions in goal-setting theory. *Current Directions in Psychological Science*, 15(5):265-268.

Lonmin Plc. 2013. *Annual report and accounts for the year ended 30 September 2013.* [Online]. http://www.zonebourse.com/LONMIN-437668/pdf/411972/LONMIN_Rapport-annuel.pdf [Accessed: 1 October 2016].

Mallin, C. 2003. *Corporate governance.* Oxford: Oxford University.

Marx, B. 2009. An analysis of audit committee responsibilities and disclosure practices at large listed companies in South Africa. *South African Journal of Accounting Research*, 23(1):31-44.

Marx, B. & Voogt, T. 2010. Audit committee responsibilities *vis-à-vis* internal audit: How well do top 40 FTSE/JSE-listed companies shape up? *Meditari Accountancy Research*, 18(1):17- 32.

Melis, A. 2005. Corporate Governance Failures: To what extent is Parmalat a particulary Italian case? *Corporate Governance: An International Review*, 13(4):478-488.

Miles, M. & Huberman, A. 1994. *Qualitative Data Analysis.* (2nd ed.) Thousand Oaks: SAGE.

Paterakis, N. & Cefaratti, M. 2014. Strenghtening audit committee communication: Internal and external audit communication guidance. *Internal Auditing,* March/April:3-7.

Public Company Accounting Oversight Board, (PCAOB). 2012. *Auditing Standard No.16*, Washington,DC: PCAOB.

Pomeranz, F. 1997. Audit committees: where do we go from here? *Managerial Auditing Journal*, 12(6):281-284.

Puth, G. 2002. *The Communicating Leader.* 2nd ed. Pretoria: Van Schaik.

Raghunandan, K., Read, W.J. & Rama, D.V. 2001. Audit committee composition, "grey directors" and interaction with internal auditing. *Accounting Horizons*, 15:105 -118.

Rashotte, L.S. 2002. "What does your smile mean? The meaning of non verbal behaviors in social interaction". *Psychology Quarterly*, March:92-102.

Republic of South Africa (RSA). 2009. *Companies Act, 71 of 2008.* Cape Town: Government Printer.

Rezaee, Z., Olibe, K.O. & Minmier, G. 2003. Improving corporate governance: The role of audit committee disclosures. *Managerial Auditing Journal*, 18(6):530-537.

Robbins, S.P. & Judge, T.A. 2013. Chapter 11 Communication. In: *Organizational Behavior.* Harlow: Pearson.

Rogelberg, S.G.; Leach, D.J.; Warr, P.B. & Burnfield, J.L. 2006. "Not another meeting!" Are meeting time demands related to employee well-being? *Journal of Applied Psychology*, 91(1): 86–96.

Rogelberg, S.G.; Scott, G. & Kello, J. 2007. The Science and Fiction of Meetings. *MIT Sloan Management Review*, Winter:18-21.

Romano, N.C. & Nunamaker, J.F. 2001. *Meeting analysis: Findings from research and practice.* HIEEE.

Scarborough, P., Rama, D.V. & Raghunandan, K. 1998. Audit committee composition and interaction with internal auditing: Canadian evidence. *Accounting Horizons*, 12:51-62.

Sekaran, U. & Bougie, R. 2013. *Elements of research design.* Chichester: John Wiley & Sons.

Shober, D. 2008. *Communicating with a vision.* Pretoria: Van Schaik.

Siegel, P. & Schultz, T. 2011. Social skills preferences among internal auditors - an explanatory study using the FIRO-B. *The Journal of Applied Business Research*, 27(3):43-54.

South Africa, 2010. *Companies Act 71 of 2008.* Claremont: Juta.

Spencer-Pickett, K.H. 2010. *The internal auditing handbook.* (3rd ed.) Chichester: John Wiley.

Tubbs, S. 2010. *Human communication: Principles and contexts.* (2th ed.) New York: McGrew-Hill.

Tuggle, C.S., Schnatterly, C.S. & Johnson, R.A. 2010. Attention patterns in the boardroom: How board composition and process affect discussion of entrepreneurial issues? *Academy of Management Journal*, 53(3):550-571.

Turley, S. & Zaman, M. 2007. Audit committee effectiveness: Informal processes and behavioural effects. *Accounting, Auditing & Accountability Journal*, 20(5):765-788.

Twala, C. 2012. The Marikana Massacre: a historical overview of the labour unrest in the mining sector in South Africa. *Southern African Peace and Security Studies*, 1(2):61- 67.

Van der Nest, D. 2008. The perceived effectiveness of audit committees in the South African public service. *Meditari Accountancy Research*, 16(2):175-188.

Volkema, R.J. & Niederman, F. 1996. Planning and managing organizational meetings: An empirical analysis of written and oral communications. *The Journal of Business Communications*, 33(3):275-296.

Watts, R. & Zimmerman, J. 1983. Agency problems, auditing, and the theory of the firm: Some evidence. *Journal of Law and Economics*, XXVI(3):613-633.

Zaman, M. & Sarens, G. 2013. Informal interactions between audit committees and internal audit functions. *Managerial Auditing Journal*, 28(6):495-515.

ANNEXURE A – INTERVIEW QUESTIONS

1 What internal audit information is included in the board packs?

2 How is this information communicated to board members?

3 What do you consider the strengths and weaknesses of the information?

4 How does the board act on this information?

5 What do you consider the strengths and weaknesses of the communication process?

6 What do you perceive to be the barriers to the communication process?

7 How do you debate controversial issues on breakdowns in the systems of internal control?

8 What is your perception of the interaction of the chairperson of the audit committee and members of the board and what attributes are needed?

An analysis of the prevalence of proper password practices among South African employees

R Butler

School of Accountancy
Stellenbosch University

ABSTRACT

When proper password practices are not applied by employees, it could pose a threat to the confidentiality, integrity and availability of an organisation's information. This study adopted a survey design to determine the password behaviour of South African computer users who access the internet from their place of employment. Based on the survey results, guidelines for proper password practices and the factors that influence password behaviour, the underlying reasons for poor password performance were investigated. It was found that South African employees' poor password performance can be attributed to a lack of knowledge of proper password practices and motivation to behave securely; an inability to convert knowledge into practice; and an over-estimation of knowledge or abilities concerning passwords. These deficiencies in password security should be addressed through appropriate education and awareness programs. This will empower employees, reduce password vulnerability and improve IT-governance within the South African context.

Key words

Computer security; passwords; passwords performance; user behaviour

1 INFORMATION SECURITY AND GOVERNANCE

Due to the pervasiveness of computer information systems, organisations are becoming increasingly dependent on these systems in their daily operations. As organisations' computer systems are also increasingly linked to other computers, networks and the internet, it increases the security risks that the computer information systems of organisations are exposed to.

Information Security encompasses three primary dimensions, namely: confidentiality, integrity and availability (ISO/IEC 2014:13). Carstens, McCauley-Bell, Malone and DeMara (2004:68) define the risks of security breaches to these dimensions as:

- breach of confidentiality – when sources not intended to have knowledge of the information is provided with this knowledge;
- breach of integrity – when unauthorized or incorrect changes are made to information; and
- breach of availability – when access is given to those who are not authorized to access the system or when those entitled to access are denied access.

In their 2014 Information Technology (IT) Security Threats and Data Breaches Survey Results Report, Kaspersky Lab (2014:4) cautions that organisations "need to be more proactive and vigilant, and they need to educate themselves – or risk becoming the next big IT security news story."

Information security threats can come from insiders (employees or former employees) as well as outsiders (such as terrorists, organised crime and hackers) (PriceWaterhouseCoopers 2015:14). Successful information security attacks can have severe negative repercussions for organisations. Unauthorized access to an organisation's system, including documents and files are password-protected, may pose risks to unauthorized access and/or changes to financial-related information about the organisation, customer or employee personal data, intellectual property, competitive intelligence, payment information and emails, theft and fraud (Kaspersky Lab 2012:20).

Nonetheless, Costin Raiu from Kaspersky Lab (2014:17) warns that after a security breach "data loss is only the tip of the financial iceberg – the true cost is much greater. There are obvious hard costs such as additional security measures and legal advice, but brand damage and reputation are arguably much larger." If customers' information is compromised in such attacks, the organisation may also be held accountable due to contravention of legislation aimed at protecting customer information, such as the Protection of Private Information (POPI) Act in South Africa. Unauthorized access to confidential information may also lead to reputational damage and a possible loss of potential future business. In addition, unauthorized access to personal customer or employee details may also create a threat to both parties from a personal perspective if such identifiable information is accessed by cyber criminals to commit identity theft (Furnell 2008:7).

All of these security threats could compromise the integrity, confidentiality and availability of an organisation's systems and the information contained in it (Posthumus & Von Solms 2004:639-640). It is, therefore, essential that organisations take the necessary steps to protect their systems and the information contained therein against such risks to prevent financial losses and/or liability.

It was the rapid development and adoption of IT, including the increasing accompanying threats that led to governance initiatives internationally and in South Africa through introducing and addressing the issue of Information Technology Governance (ITG). Today information security governance is accepted as an integral part of sound IT and Corporate Governance (Von Solms 2005:443). The principles of ITG contained in the Third King Report on Corporate Governance for South Africa (King Report) aims to protect an organisation's intellectual assets, information and IT with regard to its availability, confidentiality and integrity (King Report 2009, Principle 5.6, paragraph 42). This Report requires IT-related risks, such as information security, to form part of an organisation's risk management process (King Report, 2009, Principle 5.5). Moreover, processes and systems must be established to ensure that these risks are managed properly (King Report 2009, Principle 5.6). Various industry associations and experts such as the Information Systems Audit and Control Association (ISACA), the System Administration, Networking and Security Institute (SANS) and the National Institute of Standards and Technology (NIST) have developed control frameworks to assist organisations to address IT-related risks.

Von Solms (2005:444-445) explains that one dimension of information security governance is information security operational management, which includes both technical as well as non-technical activities. Technical activities include, *inter alia,* logical access control and identification and authentication management, which, according to Von Solms (2005:444-445), are "crucial and essential" to ensure that any IT environment is protected against risks which may affect its confidentiality, integrity and availability. Non-technical activities include, amongst others, the creation of information security policies and awareness programs to inform computer users of the risks associated with the use of IT systems, including the computer user's responsibilities in addressing IT-related risks (Von Solms 2005:445).

To protect an organisation's system and information against IT security risks it is critical that the company has processes and systems in place to identify and authenticate computer users before allowing access to systems and information. Identifying and authenticating computer users before granting access is considered the foundation of computer security (Conklin, Dietrich & Walz 2004:1). Identification refers to the process of establishing whether the computer system knows the user, while authentication involves the process to establish confidence in the validity of that user before granting access (Scarfone & Souppaya 2009:2-1).

Although other user authentication systems such as biometrics (using physical characteristics), Single-Sign-on and One-time-Pin (using device ownership), are evolving, text-based passwords as a means to identify and authenticate computer users and their access rights, whether in isolation or combination, remain the most commonly used method to control access (Shay, Komanduri, Kelley, Leon, Mazurek, Bauer, Christin & Cranor 2010:1; Stallings & Brown 2015:80; Tam, Glassman & Vandenwauver 2010: 233). This is supported by the key findings of the 2014 US State of Cybercrime survey, which indicated that 59% of the organisations surveyed use password systems to control access (PriceWaterhouseCoopers 2014:16). As the adoption and use of technology increases, having to identify oneself uniquely through a password before being allowed to perform certain actions has become acceptable, understandable and even expected in order to ensure a secure environment (Chiasson & Biddle 2007:1; Weber, Guster, Safonov & Schmidt 2008: 45).

However, password systems are susceptible to a wide range of attacks to ascertain authorized user passwords that may have negative consequences for organisations and password users personally. According to the 2014 Symantec Internet Security Threat Report, passwords were among the top 10 types of information breached in 2013 (Symantec 2014:12). Zviran and Haga (1999:164) remark that almost every attack of a computer system at some stage relies on the attacker's ability to exploit a legitimate computer user's password. Attacks to discover the passwords can occur at the system-end (where attackers launch technical or brute force attacks to crack or guess the passwords of authorized users); on the communication channel with which passwords are transmitted (by increasingly sophisticated technologies deployed at different layers of the network infrastructure); and attacks can be aimed directly at the user to discover his or her password (such as through phishing and social engineering) (Butler 2007:520; Campbell, Kleeman & Ma 2007:3; Florencio & Herley 2007:657; Notoatmodjo & Thomborson 2009:71; Zhang-Kennedy, Chiasson & Van Oorschot 2016:7).

2 PROPER PASSWORD PRACTICES AND THE COMPUTER USER

While organisations can implement technical control measures to protect their computer security against password attacks, technology can only provide a certain level of protection against some types of password attacks (Bonneau, Herley, Van Oorschot & Stajano 2015:79; Safa, Sookhak, Von Solms, Furnell, Ghani & Herawan 2015:65). Cracking or guessing passwords or tricking users into disclosing their passwords cannot be prevented by technical measures alone. Attacks on passwords can be aimed at cracking "weak" passwords as well as gaining access to all ("strong" and "weak") passwords that are not adequately protected. Consequently, using strong password characteristics when creating passwords alone will not indemnify passwords against misuse as "even a good password that is hard to guess can be unveiled" (ISACA 2010:170).

Proper password practices aim to assist in reducing the risk that cannot be controlled by technical measures alone. It refers to the policies and procedures that would enhance computer password security (Adams & Sasse 1999). The primary purpose of proper password practices is "to prevent users from choosing easy-to-guess passwords, and to guide users towards secure password management" (Zhang-Kennedy *et al* 2016:2). Therefore, these practices include a combination of measures that computer users apply when they (1) choose or create their passwords (password creation practices), and (2) keep their passwords safe once created (password management practices) (Kothari, Blythe, Smith & Koppel 2015; Zhang-Kennedy *et al* 2016:2). Although the practices of creating and managing passwords are interdependent, they are viewed as distinct for the purpose of this study, yet sharing certain actions.

Passwords used in the process to identify and authenticate users can either be system-generated automatic passwords or user-selected passwords (Scarfone & Souppaya 2009:3-8). With the introduction of new technology such as cloud based computing, which effectively removes the first barrier to access, namely physical presence, secure authentication is becoming increasingly important, irrespective of the type of password system used. In user-selected password systems, the password user has the "burden" to select strong passwords that are kept secure and confidential (Garrison 2008:70). When computer users do not select and manage their passwords with care, the computer user becomes a potential "weak link" and it may make those passwords more susceptible to potential abuse and misuse (Bonneau *et al* 2015:80). According to Tam *et al* (2010:233) even the most sophisticated security systems become useless if computer users do not select and manage their passwords properly.

The computer user's behaviour towards his/her password has a direct impact on the level of security of the computer systems and information to which that password controls access. However, while certain password users may be proficient in their password practices, reducing the security risk for the organisation, security measures and guidelines are often "unknown, neglected, or avoided" by others, which can negatively impact information security (Notoatmodjo & Thomborson 2009:71).

As the "human" element poses one of greatest information security threats to an organization's computer security, this matter needs to be addressed urgently (Alhogail, Mirza & Bakry 2015:201; Da Veiga & Eloff 2007:362). It is essential that "human" factors that influence information security is not overlooked as it influences employee security behaviour (Alhogail, *et al* 2015:201; Safa *et al* 2015:66). Researchers (Anderson & Agarwal 2010; Pfleeger & Caputo 2012; Safa *et al* 2015:66) suggest a greater understanding of the behaviour of computer users to prevent them from being the "weakest link" with regard to password security. If ignored, "organizations will not be able to protect the integrity, confidentiality and availability of information assets" (Alhogail *et al* 2015:201).

To contribute to information security and assist employees in applying proper password practices, some organisations have policies in place concerning the passwords that their employees create and use for business purposes (Shay *et al* 2010:1). In addition, the organisations' password policies (such as password composition rules) can be built into and enforced by its systems (Zhang-Kennedy *et al* 2016:2). Unfortunately, when system requirements exceed users' capabilities (when longer and more complex passwords should be chosen) or when users find them "incompatible" with the task of performing their jobs, it often diminishes the effectiveness of password systems.

Situations such as these not only reduce employee productivity but often also lead to computer users perceiving the password system as "not sensible", resulting in them circumventing the system and developing their own strategies to cope with security requirements (Inglesant & Sasse 2010:384). Moreover, in situations where no organisational policies, rules or enforcement of password practices exist, user-selected passwords may be even more vulnerable. In such instances there could be the lack of initiatives or guidance to educate and train the password user, causing computer users who are ignorant of proper password practices to employ poor password behaviour. When asked to rank the priorities of their vulnerabilities in EY's Global Information Security Survey 2014, "Careless or unaware employees" was rated as the top vulnerability by the respondents (EY 2014:4).

3 RESEARCH PROBLEM AND OBJECTIVE

Various international studies have investigated particular aspects of password behaviour among employees in various industries (including the public sector). It was revealed that poor password performance among computer users is common (Brown, Bracken, Zoccoli & Douglas 2004; Campbell *et al* 2007; Florencio & Herley 2007; Gaw & Felten 2006; Notoatmodjo & Thomborson 2009; Riley 2006; Tam *et al* 2010; Teer, Kruck & Kruck 2007; Ur, Bees, Segreti, Bauer, Christin, Cranor & Deepak 2016; Ur, Noma, Bees, Segreti, Shay, Bauer, Christin, & Cranor 2015; Wash, Rader, Berman & Wellmer 2016). However, it is unclear what the computer password security levels of South African computer users within organisations are and whether they apply safe password creation and management practices in the absence of enforced password composition rules built into an organisation's computer systems. Furthermore, limited research has been conducted to identify the "factors" that may influence safe/unsafe user behaviour among computer users (Pattinson, Parsons, Butavicius, McCormac and Calic 2016:230).

The purpose of this study is to measure the prevalence of proper password practices among South African users who access computers from their place of employment (i.e. employees) and to identify as well as establish possible reasons for unsafe behaviour. Research conducted by Pattinson *et al* (2016) revealed that organisations can reduce information security risks through the implementation of appropriate intervention

strategies that take into account any areas of poor human security behaviour by employees. The deficiencies in password performance highlighted by this research could identify areas where relevant intervention programs should focus. The US State of Cybercrime Survey for 2014 (PriceWaterhouse Coopers 2014) found that organisations spent less on security incidents when employees are properly trained in security-related matters.

Suitable employee training and awareness should be included as a fundamental component of an organisation's information security initiatives to improve users' security behaviour (PriceWaterhouseCoopers 2015:27; Safa *et al* 2015:67). The findings of this study must be considered by organisations when developing passwords security training and awareness programs or when establishing password policies and rules for that organisation. This will improve the password behaviour of employees, leading to improved IT security within the organisation.

4 DESIGN AND METHODOLOGY

A survey design was deemed appropriate to answer the research problem. A survey consists of a predetermined set of questions distributed to representatives of the larger population of interest (Shaughnessy, Zechmeister & Jeanne 2011). The survey was designed and administered using an online platform, which given the nature of the topic (password behaviour of users), was deemed appropriate.

The survey was designed after an extensive literature review was undertaken to determine the guidelines for proper password practices and factors that influence users' password behaviour. The guidelines for proper password creation and management were based on the literature review and summarised in Table 1. The factors that influence users' password behaviour were investigated to establish the factors that may influence password performance. A password behaviour construct was developed based on this process (refer to Figure 1).

To determine the computer password behaviour of South African employees, the information obtained in the abovementioned process was used to design a survey to establish the following:

- Perception: The perception of South African employees about their password creation and management knowledge and abilities.
- Reality: The password practices that the employees generally apply when they create and manage their passwords.
- Password distinction ability: Password users' ability to distinguish between more and less secure passwords.

The results from the survey were compared to the guidelines for proper password practices to determine areas of deficiency. Based on the results of this study, the areas of and possible reasons for poor password behaviour among South African employees who have to create and manage passwords was determined. This is diagrammatically presented in Figure 2.

4.1 Guidelines for proper password creation and management

The Password Management Guideline, published by the Department of Defence Computer Security Centre in 1985, forms the basis of a set of 'standard' password rules that was developed and recommended over time by researchers and industry associations (Cheswick, 2013:41). However, as password security concerns and threats have evolved significantly in recent years, researchers have begun to question the appropriateness of the 'standard' password creation and management rules (Cheswick, 2013; Zhang-Kennedy *et al* 2016). Zhang-Kennedy *et al* (2016) conducted a study to determine which of the traditional password rules are still appropriate, taking into account the types and levels of sophistication of security threats that user-selected passwords are exposed to today. They also considered the potential security benefits and usability cost of the 'standard' password practices and created an 'updated' set of password rules (Zhang-Kennedy *et al* 2016).

Taking into account the discussions above, guidelines for proper password creation and management as determined through the literature review are summarised in Table 1.

4.2 Factors that influence password performance

The password performance of computer users differ because their behaviour is influenced by a number of aspects (McCloy, Campbell & Cudeck 1994:493). According to Heider (1958) (as cited in Anderson & Butzin 1974:598), an individual's performance in a particular task is influenced by the individual's ability and motivation to perform that task. Heider's function for performance was refined by McCloy *et al* (1994) who defines ability as a combination of the knowledge, skills and competencies that enable a human to perform a particular task (McCloy *et al* 1994:494).

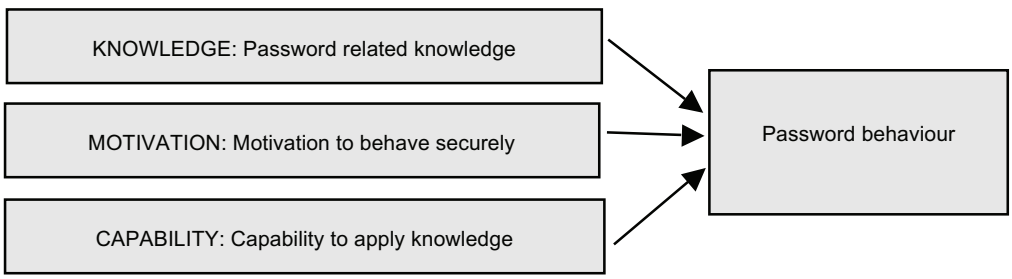
These researchers further identified that both the knowledge of facts, rules, principles and procedures relating to a task (declarative knowledge) as well as the user's capability when his/her knowledge has been successfully combined with knowing how and being able to perform that task (procedural knowledge and skills) and motivation influence an individual's performance. These authors further assert that motivation refers to the underlying drive behind a user's particular behaviour in performing that task, which can be influenced by the user's desire to extend effort, the intensity of the effort, as well as the user's commitment in extending effort (McCloy *et al* 1994:494).

Table 1: Guidelines for proper password practices

Password practice	Explanation
Security should be a foremost concern when creating new passwords (Huth, Orlando & Pesante 2012; ISACA 2010; Singleton 2012; Zhang-Kennedy *et al* 2016).	Password security and its vulnerability should be a primary concern when creating new passwords. "Strength" of passwords should be more important than the "ease of remembering" that password for future use.
Uniqueness (Allan 2012; Bonneau *et al* 2015; Garrison 2008; ISACA 2010; SANS 2014; Zhang-Kennedy *et al* 2016).	Unique passwords should be used for all accounts, especially high risk accounts. Re-using old passwords or variations of past passwords increase their vulnerability. One password should not be used simultaneously for more than one account or site, as this may lead to unauthorized access to multiple accounts when these passwords are discovered.
Vary complexity with the risk associated (Bonneau *et al* 2015; Brown *et al* 2004; ISACA 2008; Zhang-Kennedy *et al* 2016).	The complexity of a password should be varied to match the purpose of the password, taking into account the risk associated with its use. More secure passwords should be chosen for higher risk purposes, such as for internet banking.
Use non-personal information and uncommon information (Allan 2012; Furnell 2007; Garrison 2008; Singleton 2012; Turan, Barker, Burr & Chen 2010; Zhang-Kennedy *et al* 2016).	Personal information or any aspect that may be associated with the computer user (such as names, nicknames, telephone numbers, dates of birth, pet's name, favourite colour) should not be used when creating passwords. This makes passwords easier to guess. Common words that appears in dictionaries as well as well-known phrases should be avoided.
Use a combination of characters when creating passwords (Allan 2012; Bonneau *et al* 2015; Brown *et al* 2004; Scarfone & Souppaya 2009; Shay *et al* 2010; Singleton 2012; Turan *et al* 2010; Zhang-Kennedy *et al* 2016).	A combination of alphabetical (both upper and lower case) and numerical characters should be used and special characters should be included for increased security. Letters sequential in the alphabet, sequential numbers or letters (such as "123456"), numbers or symbols consecutive on keyboards (such as "QWERTY") should not be used when creating passwords. Alphabetical characters in passwords may be substituted with similar looking numerical characters, such as using the "0" instead of the "o" to make them more complex.
Choose longer passwords that are more secure (Allan 2012; Bonneau *et al* 2015; Campbell *et al* 2007; Furnell 2007; Garrison 2008; Singleton 2012; Wakefield 2004; Zhang-Kennedy *et al* 2016).	Passwords of at least eight characters long should be used to increase its complexity and make it more difficult to crack.
Be cautious when sharing or disclosing passwords (Allan 2012; Butler 2007; Furnell 2007; McDowell, Hernan & Rafail 2013; ISACA 2010; SANS 2014; Zhang-Kennedy *et al* 2016).	Passwords should be kept secret and not be disclosed to or shared with others. This increases their confidentiality and decreases the possibility of the passwords being discovered or misused.
Store passwords securely (Allan 2012; Bonneau *et al* 2015; SANS 2014; Wakefield 2004; Zhang-Kennedy *et al* 2016).	Keep passwords protected. Preferably, passwords should not be written-down or kept in places where they may easily be discovered. When storing passwords in an electronic format ensure that the file is password-protected.
Change passwords regularly and when it is suspected that a service was compromised (Adams & Sasse 1999; Allan 2012; Furnell 2007; SANS 2014; Zhang-Kennedy *et al* 2016).	Change passwords regularly. The shorter the lifetime of a password the better, as it reduces the risk of undetected compromised passwords. Passwords should be changed after a security breach.

When applying the factors that influence human behaviour to that of a user's behaviour concerning passwords, a computer user's password behaviour is influenced by three aspects (refer to Figure 1), namely (1) that user's password related-knowledge; (2) the motivation behind the user's password behaviour (i.e. whether the user is concerned with password security or not); and (3) the user's capability to distinguish between more and less secure passwords and the ability to apply proper password practices.

Figure 1: Password behaviour construct used in this study (Author's own construct)



According to Michie, Johnston, Francis, Hardeman and Eccles (2008), targeting the determinants of behaviour represents a way to achieve behavioural change. It should, therefore, be possible to improve

the overall password performance of South African employees if any deficiencies in the three determinants of password behaviour is identified and addressed. This can only be achieved once the password behaviour among South African employees is established and the presence of the factors that influence password behaviour is analysed.

4.3 Survey

The survey comprised of 43 structured and open-ended questions. It was designed and refined using two iterations of pilot testing. Care was taken to ensure respondents that their passwords would not be requested and that the purpose of the study was to merely gather information on the practices that users apply.

Perceptions and reality
The survey contained direct questions aimed at determining the respondents' perception of and knowledge about password-related matters as well as their password creation and management practices. Their perceptions were compared with the practices that they apply (reality) to determine correlation.

Password distinction ability
The survey also contained a section where the respondents were provided with a set of passwords and were required to indicate which passwords they deem more or less secure – hereafter referred to as the 'password distinction test'.

The passwords provided in the survey tested various aspects of password security, including the combination of characters used in the composition of the password (e.g. including uppercase letters as opposed to only using lowercase letters, including numerical characters as opposed to only using alphabetical characters as well as including special characters), using dictionary versus non-dictionary words, the use of longer versus shorter passwords and using inflections of words instead of merely the root form of a word.

The survey contained six questions in which two passwords were provided in each. The respondents were required to indicate whether they deemed the one or the other password more secure, whether the two passwords were equally secure or whether they did not know. In three additional questions, the respondents had to rank five passwords that were provided in each question from the most to the least secure. The strength of the passwords provided in the survey were tested against various passwords strength meters. Based on the respondents' classification of the passwords, a measured password distinction ability score (MPDA) was calculated for each respondent.

The study used the survey questions as well as the password distinction test to test for the prevalence of proper password practices among South African employees (refer to Table 2).

Table 2: Methodology used for testing the prevalence of proper password practices

Password practice	How tested in this study
Security should be the foremost concern when creating passwords.	Survey question.
Use unique passwords that are not used for other purposes.	Survey question.
Vary complexity with risk.	Survey question.
Use non-personal information when creating passwords.	Survey question and Password distinction test.
Use a combination of upper- and lowercase letters as well as numbers.	Survey question and Password distinction test.
Longer passwords are more secure.	Survey question and Password distinction test.
Don't share or disclose passwords.	Survey question.
Store passwords securely.	Survey question.
Change passwords regularly.	Survey question.

The survey was not conducted among employees at a particular employer organisation. As access to the internet increases the information security risk for an organisation, a computer connected to the internet as well as for any other computers, systems and networks connected to it, the password behaviour of respondents who indicated that they *accessed the internet* (for various purposes) *from a computer at their place of employment* were analysed further to determine how these respondents (who are employees) create and manage passwords.

5 FINDINGS

5.1 Demographics and internet usage

Besides their place of employment, the users also access the internet from other locations as depicted in Table 3.

Of the 609 South African respondents who access the internet from their place of employment, and whose responses were further analysed for the purpose of this study, 50% were female and 50% male. Apart from the traditional security risks arising when a user connects to the internet, accessing organisational computers and information via mobile devices, making use of WiFi networks and internet cafes increases this risk for their employer organisation's computer system.

Fewer than 4% of the respondents indicated that they use system generated passwords, which implies that more than 96% of the respondents have been subjected to the creation and management of passwords when interacting with the internet. Users have to create and manage numerous passwords, as inferred when asked about the number of sites the respondents visit that require authentication.

Identification and authentication is applicable to 84% of the respondents who visit at least five sites, while 47% of the respondents visit ten or more sites requiring authentication.

Table 3: Locations from where the internet is accessed

Location	Number of respondents	Location	Number of respondents
Residential home	582	Coffee shop with WiFi	207
Place of employment	609	Educational institution	143
Constant mobile access	361	Internet café	63
Wherever WiFi is available	269	Other	15

Respondents are active internet users, using the internet for a wide range of activities, predominantly for Financial Services and Communication (98%), Communication (97%) News and Information (89%) and Social Networking (83%). Employees who access the internet from their place of employment increases the vulnerability of an organisation's information security.

5.2 Perception versus reality

When comparing employees' perception regarding their password abilities to the password creation and management practices that they do apply, the following disparities were evident:

- A lack of knowledge about proper password practices: 65% of the respondents were not exactly sure what "strong" passwords were.
- Respondents often overestimate their knowledge and ability or underestimate their vulnerability or are unable to apply the knowledge that they do possess in the practices that they apply:
  - When analysing the survey results, almost 6% of the respondents perceived that they possess absolute knowledge of password practices. However, only a single respondent demonstrated flawless capability to apply proper password creation and management practices as measured in this study.
  - While more than 78% of the respondents felt comfortable with their password creation and management practices, numerous instances of poor password practices were displayed. These are discussed in Section 5.3.
  - Only 11% of the respondents were able to correctly rank the strength of all the passwords provided in the password distinction test (obtained a MPDA of 100%), despite 35% of the respondents indicating that they "knew exactly" and 46% having "a very good idea" what is meant by a strong password.

5.3 Prevalence of proper password practices

This section describes the survey results including the results of the subsequent analysis into the prevalence of proper password practices (as summarised in Table 1) among South African employee password users.

Security should be the foremost concern when creating passwords

Only 3% of the respondents displayed a perfect "security first" aptitude when selecting and managing passwords. When creating passwords, convenience is more important to many users than its security. The respondents indicated that "ease of remembering" the password was more important (44%) than the "strength" of passwords (33%). One-third of the respondents held that the internet is generally safe and too much fuss is being made about the risks associated with it, which revealed a lack of security-consciousness.

Use unique passwords that are not used for other purposes

Re-using passwords (79%) and the simultaneous use of a password for more than one purpose (91%) are common practices among respondents. An alarming 20% of the respondents indicated that they use their current internet banking password to also access other sites. Re-using passwords and using variations of past passwords were evident even regarding respondents' internet banking passwords, which is a high risk account.

Vary complexity with risk

It was clear that the respondents do not consider the purpose of the password and the risk associated with its use when creating new passwords. The "perceived risk associated with the site" was the most important consideration for only 18% of the respondents. Only 17% of the respondents rated it the second most important aspect when creating new passwords.

Use non-personal information and uncommon information when creating passwords

The difficulty to remember passwords was experienced by 86% of the respondents. The struggle to remember passwords increases the use of unsafe practices. "Ease of remembering" was signified by 44% of the respondents as the foremost concern when choosing new passwords while the second most important aspect by 22% of the respondents.

When creating new passwords, personally meaningful words (72%) and meaningful numbers (61%) are primary mechanisms employed by respondents to remember passwords.

In the password distinction test, 95% of the respondents were able to identify that the password that was a non-dictionary word is more secure than common dictionary words.

Use a combination of uppercase and lowercase letters as well as numbers

Although certain respondents indicated that they use a combination of upper and lower case alphabetical characters, numerical characters and special characters when creating new passwords, 43% of the respondents do not use a combination of

alphabetical-, numerical- and special characters when creating passwords.

Other weak practices included using only alphabetical characters (5%), numerical characters (1%), upper case (3%) and lower case characters (14%), using numerical and lower case letters (no capital letters) (11%), numerical and capital letters (no lower case letters) (3%), letters sequential in the alphabet (3%), sequential numbers (10%), letters consecutive on keyboards (4%), numbers consecutive on keyboards (4%) and symbols consecutive on keyboards (4%).

In the password distinction ability test, the respondents correctly identified passwords containing an upper case letter (82%), a number (97%), a non-dictionary word (95%) and special characters (95%) were more secure than those consisting of only lower case letters, no numbers, and common dictionary words that contained no special characters.

However, it was clear that while the respondents found it relatively easy to choose the more secure of the two passwords, arranging five passwords that tested a combination of password characteristics from most to least secure proved more complex. In a question where adding numerical characters to words, using a non-dictionary word, a password consisting of only numerical characters and a password consisting of mixed random letters, numbers and special characters, fewer than 20% of the respondents were able to classify the passwords correctly from most to least secure.

Choose longer passwords that are more secure
One of the positive aspects was that fewer than 10% of the respondents indicated that passwords that are "short and easy to enter" was the most important or second most important aspect when creating new passwords.

In the password distinction ability test, the respondents were able to identify that the longer password containing an inflection of a word were more secure than the shorter one (69%).

Don't share or disclose passwords
Password sharing is common among South African users. A total of 53% of the respondents have shared at least one password with another person, while 53% are familiar with the password to an account or system that is not their own.

Store passwords securely
Weak practices applied to remember passwords include keeping a list/record thereof (30%), storing passwords in an electronic non-password-protected format (14%) and have their browser keep track of their passwords (20%). Only 7% use password management software to store passwords safely.

Change passwords regularly
Although 70% of the respondents are aware of the need to change their passwords regularly, 23% indicated that they do so frequently. A total of 68% of the respondents who utilise internet banking had not changed their internet banking password in the last year while 49% not within the last two years.

The respondents did not change their internet banking passwords when they became aware of security breaches in the media (47%), personally suffered security breaches (2%), learnt about their friends, family or colleagues' bad experiences (28%) or the realisation that their current password was insecure (15%). The respondents also indicated that even when they suffer future personal losses, they would not change their internet banking passwords (2%).

The majority of the respondents indicated that they only change passwords when the system force them to do so. Moreover, they re-used the passwords or affected variations thereto, even for high risk environments.

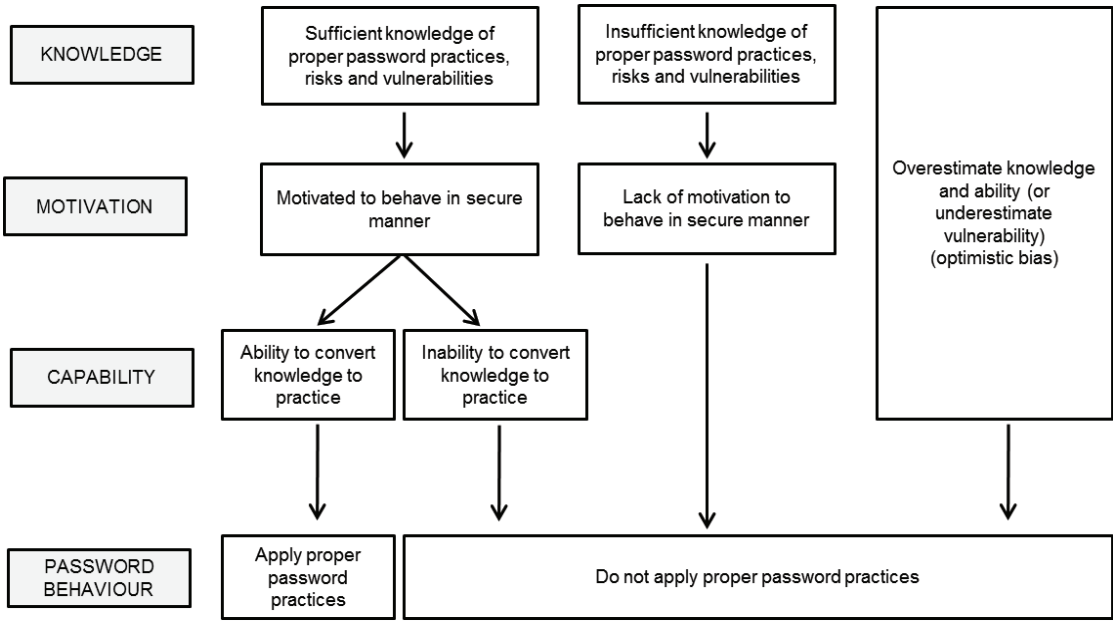
6 REASONS FOR POOR PASSWORDS BEHAVIOUR

Based on the incidence of poor password behaviour that was evident when assessing the prevalence of proper password practices and considering the Password behaviour construct that was used in this study (refer to Figure 1), three reasons that contribute towards computer users' poor password performance are identified, namely: (1) a lack of knowledge of proper password practices, risk and vulnerabilities and motivation to behave securely; (2) the inability to convert knowledge into practice due to a lack of the necessary knowledge and motivation; and (3) an over-estimation of their knowledge or abilities concerning passwords (or underestimation of their vulnerability). This is diagrammatically presented in Figure 2.

6.1 Lack of knowledge and security-motivation

Many employees lack the necessary password-related skills and knowledge to be proficient password users (Alhogail *et al* 2015:202). Furnell (2007:445) established that many computer users do not apply safe password practices because "they may not know any better" due to a lack of appropriate knowledge, guidance and support. This was confirmed by Adams and Sasse (1999:42) who established that password users possessed inadequate knowledge, which resulted in users who "make up their own rules" as a result of thereof. Various researchers (Adams & Sasse 1999:43 & 46; Conklin *et al* 2004:5; Riley 2006) have found that users often lack knowledge of proper password practices, security risks, users' vulnerability and possible consequences to the parties involved. Due to their ignorance, these users create "weak" passwords and/or manage their passwords improperly (irrespective of whether they are "weak" or "strong") and/or engage in more risky behaviour.

Figure 2: Possible reasons for users' poor password performance (Author's own construct)



6.2 Inability to apply knowledge

Certain computer users may have the required password-related knowledge but fail to display it in their behaviour. Studies by Riley (2006), Tam *et al* (2010) and Wessels and Steenkamp (2007) revealed that even users with the ability to distinguish between secure and insure practices often don't apply secure practices. This inability could stem from a lack of awareness of their vulnerability and the possible consequences related to poor password behaviour (Gaw & Felten 2006:45) or users' inherent carelessness or negligence (Safa *et al* 2015:66). Another reason could be that users suffer from "password overload" and apply unsafe practices because they struggle to remember their passwords when creating numerous "strong" passwords that are kept safe (Bonneau *et al* 2015:83; Notoatmodjo & Thomborson, 2009:71; Zhang-Kennedy *et al* 2016:1). To manage the memory challenge, users devise their own "unsafe" methods to remember passwords, including using short and weak passwords that are easy to recall, sharing passwords, writing down passwords and re-using passwords (Bonneau *et al* 2015: 84; Campbell *et al* 2007:3; Carstens *et al* 2004:74).

6.3 Over-confidence in knowledge and abilities

A further reason why users apply unsafe practices could be the overestimation of their knowledge and ability regarding password practices or underestimation of their vulnerability due to a phenomenon known as "optimistic bias" or "unrealistic optimism" (Weinstein 1980:806). This results in users who overestimate their ability to create "strong" passwords that are properly managed and protected, and/or underestimate the potential risk associated with their behaviour and compromised passwords. This misconception results in many users believing that attackers would not be able to guess or discover their passwords (Chiasson & Biddle 2007:2).

7 CONCLUSION

Users' password behaviour has a direct impact on the level of computer security of the system these passwords control access to. When computer users have to create and manage user-selected passwords, they often apply unsafe password practices, as illustrated by this and various international studies, which make passwords more vulnerable to attacks. User-selected password systems remain a threat to an organisation's computer security when proper password creation and management practices are not applied by an organisation's computer users.

It is evident from this study that South African employees do not always apply proper password practices. Although a clear lack of password-related knowledge is evident from this study, the results revealed a willingness among respondents to improve their password practices if they had more knowledge on password-related matters or were made aware that they had utilised unsafe practices. 53% of the respondents indicated that they will definitely, while 36% stated that they may change their passwords if they realized that the current one was insecure. An overwhelming 73% of the respondents indicated that they would like to receive a copy of the guidelines for safer online password practices that are to be compiled and distributed based on this research in an effort to improve their password behaviour.

To improve password performance, one of the most common suggestions made by researchers is improved, suitable security education, training and awareness programs (Adams & Sasse 1999:43 & 46; Butler 2007:250; Conklin *et al* 2004:5; Furnell, Bryant & Phippen 2007:417; Riley 2006; Safa *et al* 2015:67). Relevant education and awareness programs that focus on areas where a lack of secure behaviour by employees exists, can empower computer users to reduce the vulnerability of their passwords (Kortjan & Von Solms 2014; Pattinson *et al* 2016:229).

Once organisations establish deficiencies in their employees' password behaviour, it is vital that awareness and educational programs aimed directly at changing the employees' attitude and behaviour towards password security be introduced to improve employees' password behaviour. When users are not informed about the improper application of password practices, they may continue to apply unsafe practices thereby increasing the vulnerability of the password system even further. Without the necessary guidance and education, password users may not be able to improve their computer password security. Computer users often take "an ostrich-like attitude" towards computer security, underestimating the vulnerability created by their actions, believing that there is "little that they can do" to protect the organisation's information asset against security threats (Cone, Irvine, Thompson & Nguyen 2007:63).

It is necessary that organisations develop and implement suitable awareness and educational programs, including providing users with guidelines for safer password practices to improve computer password security. Such initiatives will (1) assist employees to identify when they apply unsafe practices; and (2) serve as a guideline to improve their password practices because users often lack the required knowledge of proper password practices. These guidelines will improve employees' computer password security knowledge, contribute to their ability and motivation to apply safe password practices when using the organisation's access control system. By improving computer password security, organisations will improve ITG and reduce the threat to the confidentiality, integrity and availability of the organisation's systems and the information contained therein.

REFERENCES

Adams, A. & Sasse, M.A. 1999. Users are not the enemy. *Communications of the ACM*, 42(12):40-46.

Alhogail, A., Mirza, A. & Bakry, S.H. 2015. A comprehensive human factor framework for Information Security in organizations. *Journal of Theoretical and Applied Information Technology*, 78(2):201-211.

Allan, A. 2012. *Best Practices for Managing Passwords: End-User Policies must balance Risk, Compliance and Usability Needs, 2012 Update,* [Online]. http://www.gartner.com/document/2012016?ref=solrAll&refval=172525021&qid=9dfc04c8a00620c1959fe382e2ca1c23 (Accessed: August 2016).

Anderson, C.L. & Agarwal, R. 2010. Practicing safe computing: a multimedia empirical examination of home computer user security behavioral intentions. *MIS Quarterly*, 34(3):613-643.

Anderson, N.H. & Butzin, C.A. 1974. Performance = Motivation × Ability: An integration-theoretical analysis. *Journal of personality and social psychology,* 30(5):598-604.

Bonneau, J., Herley, C., van Oorschot, P.C. & Stajano, F. 2015. Passwords and the evolution of imperfect authentication. *Communications of the ACM,* 58(7):78-87.

Brown, A.S., Bracken, E., Zoccoli, S. & Douglas, K. 2004. Generating and remembering passwords. *Applied Cognitive Psychology*, 18(6):641-651.

Butler, R. 2007. A framework of anti-phishing measures aimed at protecting the online consumer's identity. *The Electronic Library*, 25(5):517-533.

Campbell, J., Kleeman, D. & Ma, W. 2007. The good and not so good of enforcing password composition rules. *Information Systems Security*, 16(1):2-8.

Carstens, D.S., McCauley-Bell, P.R., Malone, L.C. & DeMara, R.F. 2004. Evaluation of the human impact of password authentication practices on information security. *Informing Science: International Journal of an Emerging Transdiscipline*, 7:67-85.

Cheswick, W. 2013. Rethinking passwords. *Communications of the ACM*, 56(2):40-44.

Chiasson, S. & Biddle, R. 2007. *Issues in User Authentication*. CHI Workshop Security User Studies Methodologies and Best Practices, San Jose, California, April, 2007.

Cone, B.D., Irvine, C.E., Thompson, M.F. & Nguyen, T.D. 2007. A video game for cyber security training and awareness. *Computers & Security*, 26(1):63-72.

Conklin, A., Dietrich, G. & Walz, D. 2004. Password-based authentication: a system perspective. *Proceedings of the 37th Annual Hawaii International Conference on System Sciences*, Hawaii, January:1-10.

Da Veiga, A. & Eloff, J.H.P. 2007. An Information Security Governance Framework. *Information Systems Management*, 24(4):361-372.

EY. 2014. *Get ahead of cybercrime – EY's Global Information Security Survey 2014*, [Online]. http://www.ey.com/Publication/vwLUAssets/EY-global-information-security-survey-2014/$FILE/EY-global-information-security-survey-2014.pdf (Accessed: August 2015).

Florencio, D. & Herley, C. 2007. A large-scale study of web password habits. *Proceedings of the 16th international conference on World Wide Web*, ACM, Banff, Canada, May:657-666.

Furnell, S. 2007. An assessment of website password practices. *Computers & Security*, 26(7):445-451.

Furnell, S. 2008. End-user security culture: A lesson that will never be learnt? *Computer Fraud & Security*, 2008(4):6-9.

Furnell, S., Bryant, P. & Phippen, A.D. 2007. Assessing the security perceptions of personal Internet users, *Computers & Security*, 26(5):410-417.

Garrison, C.P. 2008. An evaluation of passwords. *Online CPA Journal,* May:70-71.

Gaw, S. & Felten, E.W. 2006. Password management strategies for online accounts. *Proceedings of the second symposium on Usable privacy and security,* ACM, Pittsburgh, P.A., July:44-55.

Huth, A., Orlando, M. & Pesante, L. 2012. Password security, protection, and management. *United States Computer Emergency Readiness Team*, [Online]. https://www.us-cert.gov/sites/default/files/publications/PasswordMgmt2012.pdf (Accessed: November 2015).

Information Systems Audit and Control Association (ISACA). 2008. *Information Security Governance: Guidance for Information Security Managers,* [Online]. http://www.isaca.org/Knowledge-Center/Research/Documents/InfoSec-Guidance-for-Information-Security-Managers_res_Eng_0508.pdf (Accessed: August 2016).

Information Systems Audit and Control Association (ISACA). 2010*. IT Standards, Guidelines and Tools and Techniques for Audit and Assurance and Control Professionals*, [Online]. http://www.isaca.org/Education/Training/On-Site-Training/Documents/ALL-IT-Standards-Guidelines-and-Tools.pdf (Accessed: August 2016).

Inglesant, P.G. & Sasse, M.A. 2010. The true cost of unusable password policies: password use in the wild. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ACM, Atlanta, Georgia, April, 2010, pp. 383-392.

International Organization for Standardization and International Electrotechnical Commission (ISO/IEC). 2014. ISO/IEC 27000. Information technology – Security *techniques – Information security management systems – Overview and vocabulary,* [Online]. http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html (Accessed: July 2014).

Kaspersky Lab. 2012. Global IT Security Risks 2012. *Kaspersky Lab,* [Online]. http://www.kaspersky.com/downloads/pdf/kaspersky_global_it-security-risks-survey_report_eng_final.pdf (Accessed: August 2015).

Kaspersky Lab. 2014. Exclusive 2014 Survey Results – IT Security Threats and Data Breaches: Perception versus Reality: Time to Recalibrate. *Kaspersky Lab,* [Online]. http://media.kaspersky.com/en/business-security/Global-IT-Risks-Report-2014-Threat-Security-Data-Breaches.pdf (Accessed: August 2015).

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

Kortjan, N. & Von Solms, R. 2014. A conceptual framework for cyber-security awareness and education in SA. *South African Computer Journal*, 52:29-41.

Kothari, V., Blythe, J., Smith, S. W. & Koppel, R. 2015. Measuring the security impacts of password policies using cognitive behavioral agent-based modelling. *Proceedings of the 2015 Symposium and Bootcamp on the Science of Security*, Urbana, I.L., April:13-22.

McCloy, R.A., Campbell, J.P. & Cudeck, R. 1994. A confirmatory test of a model of performance determinants. *Journal of Applied Psychology*, 79(4):493-505.

McDowell, M., Hernan, S. & Rafail, J. 2013. Choosing and Protecting Passwords. *United States Computer Emergency Readiness Team*, [Online]. https://www.us-cert.gov/ncas/tips/ST04-002 (Accessed: April 2016).

Michie, S., Johnston, M., Francis, J., Hardeman, W. & Eccles, M. 2008. From Theory to Intervention: Mapping Theoretically Derived Behavioural Determinants to Behaviour Change Techniques. *Applied Psychology: An International Review*, 57(4):660-680.

Notoatmodjo, G. & Thomborson, C. 2009. Passwords and perceptions. *Proceedings of the Seventh Australasian Conference on Information Security,* Australian Computer Society Inc., Wellington, New Zealand, January, 2009, 98:71-78.

Pattinson, M., Parsons, K., Butavicius, M., McCormac, A. & Calic, D. 2016. Assessing Information Security Attitudes: A comparison of two studies. *Information & Computer Security*, 24(2):228-240.

Pfleeger, S.L. & Caputo, D.D. 2012. Leveraging behavioral science to mitigate cyber security risk. *Computers & Security*, 31(4):597-611.

Posthumus, S. & Von Solms, R. 2004. A framework for the governance of information security, *Computers & Security*, 23(8):638-646.

PriceWaterhouseCoopers. 2014. US Cybercrime: Rising risks, reduced readiness – Key finds from the 2014 US State of Cybercrime Survey. *PriceWaterhouseCoopers*, [Online]. http://www.pwc.com/en_US/us/increasing-it-effectiveness/publications/assets/pwc-2014-us-state-of-cybercrime.pdf (Accessed: August 2015).

PriceWaterhouseCoopers. 2015. The Global State of Information Security Survey – 2015. *PriceWaterhouseCoopers*, [Online]. http://www.pwc.com/gx/en/consulting-services/information-security-survey (Accessed: August 2015).

Riley, S. 2006. Password security: What users know and what they actually do. *Usability News*, 8(1):2833-2836.

Safa, N.S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N.A. & Herawan, T. 2015. Information security conscious care behaviour formation in organizations. *Computers & Security*, 53:65-78.

Scarfone, K. & Souppaya, M. 2009. *Guide to enterprise password management - Special Publication 800-188 (Draft).* National Institute of Standards and Technology (NIST), US Department of Commerce, [Online]. http://csrc.nist.gov/publications/drafts/800-118/draft-sp800-118.pdf (Accessed: August 2015).

Shaughnessy, J., Zechmeister, E. & Jeanne, Z. 2011. *Research methods in psychology*. 9th edition. New York, NY: McGraw Hill, pp. 161–175.

Shay, R., Komanduri, S., Kelley, P.G., Leon, P.G., Mazurek, M.L., Bauer, L., Christin, N. & Cranor, L.F. 2010. Encountering stronger password requirements: user attitudes and behaviors. *Proceedings of the Sixth Symposium on Usable Privacy and Security,* ACM, Redmond, W.A., July.

Singleton, T.W. 2012. Evaluating Access Controls Over Data. *ISACA Journal*, 1.

Stallings, W. & Brown, L. 2015. *Computer Security Principles and Practice*. Upper Saddle River, New Jersey: Pearson.

Symantec. 2014. *Internet Security Threat Report*, [Online]. http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf (Accessed: April 2016).

System Administration, Networking and Security Institute (SANS), 2014. *Password protection policy*, [Online]. https://www.sans.org/security-resources/policies/general/pdf/password-protection-policy (Accessed: August 2016).

Tam, L., Glassman, M. & Vandenwauver, M. 2010. The psychology of password management: a tradeoff between security and convenience. *Behaviour & Information Technology*, 29(3):233-244.

Teer, F.P., Kruck, S. & Kruck, G.P. 2007. Empirical study of Students' Computer Security Practices/Perceptions. *Journal of Computer Information Systems*, 47(3):105-110.

Turan, M., Barker, E., Burr, W. & Chen, L. 2010. *Recommendation for password-based key derivation - Special publication 800-132. National Institute of Standards and Technology (NIST), US Department of Commerce, Computer Security Division, Information Technology Laboratory,* [Online]. http://csrc.nist.gov/publications/nistpubs/800-132/nist-sp800-132.pdf (Accessed: September 2015).

Ur, B., Bees, J., Segreti, S.M., Bauer, L., Christin, N., Cranor, L.F. & Deepak, A. 2016. Do Users' Perceptions of Password Security Match Reality? *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, San Jose, CA, May, 2016.

Ur, B., Noma, F., Bees, J., Segreti, S.M., Shay, R., Bauer, L., Christin, N. & Cranor, L.F. 2015. I Added'!'at the End to Make It Secure: Observing Password Creation in the Lab. *Proceedings of the Eleventh Symposium On Usable Privacy and Security*, Ottawa, Canada, July:123-140.

Von Solms, S.H. 2005. Information Security Governance - Compliance management vs operational management. *Computers & Security*, 24(6):443-447.

Wakefield, R.L. 2004. Network security and password policies. *The CPA Journal*, 74(7):6-8.

Wash, R., Rader, E., Berman, R. & Wellmer, Z. 2016. Understanding Password Choices: How Frequently Entered Passwords are Re-used Across Websites. *Proceedings of the Symposium on Usable Privacy and Security*, Denver, Colorado, June, 2016.

Weber, J.E., Guster, D., Safonov, P. & Schmidt, M.B. 2008. Weak password security: An empirical study. *Information Security Journal: A Global Perspective*, 17(1):45-54.

Weinstein, N.D. 1980. Unrealistic optimism about future life events. *Journal of personality and social psychology*, 39(5):806-820.

Wessels, P. & Steenkamp, L. 2007. Assessment of current practices in creating and using passwords as a control mechanism for information access. *South African Journal of Information Management,* 9(2):1-17.

Zhang-Kennedy, L., Chiasson, S. & Van Oorschot, P. 2016. Revisiting password rules: facilitating human management of passwords. *Proceedings of the 2016 APWG Symposium on Electronic Crime Research (eCrime)*, Toronto, Canada, June, 2016.

Zviran, M. & Haga, W.J. 1999. Password security: an empirical study. *Journal of Management Information Systems,* 15(4):161-185.

The Southern African Journal of Accountability and Auditing Research

Evolving Research

Blowing the whistle for personal gain in the Republic of South Africa: An option for consideration in the fight against fraud?

S Lubisi
Department of Auditing
University of Pretoria

H Bezuidenhout
Department of Auditing
University of Pretoria

ABSTRACT

Financially rewarding whistleblowers for information that has led to recovery of fraud losses suffered by government is common practice under the United States of America's False Claims Act of 1986. However, a whistleblower in the Republic of South Africa is not afforded similar treatment in terms of section 9(1)(b) of the Protected Disclosures Act (26 of 2000) of the Republic of South Africa. In certain circumstances, whistleblowers may not even be protected against occupational detriment resulting from the disclosure. Similar principles of the Protected Disclosures Act in terms of rewarding whistleblowers also apply in the United Kingdom. The objective of this article is to establish whether rewarding whistleblowers should be considered in the fight against fraud in the Republic of South Africa with a similar view of the United States of America's False Claims Act. In order to address the research objective, the adopted methodology can be described as a conceptual review of whistleblowing policies and regulations in the public sector, specifically focusing on rewarding whistleblowers. This article, therefore, evaluates available literature to determine whether the Republic of South Africa should consider the False Claims Act route by reviewing its legal position, United States of America and the United Kingdom. It further considers whistleblowing as a fraud risk management tool and raises the question whether the current legal obligations on public officials to report fraud are effective in curbing it.

Key words

Whistleblowing; whistleblower rewards; Protected Disclosures Act 26 of 2000; fraud risk management; False Claims Act

1 INTRODUCTION AND BACKGROUND

The pandemic of fraud and corruption is problematic; it obstructs economic growth, public trust, and undermines the values of democracy (Botha & Van Heerden 2014:Online; Diale 2005:Online). It also brings with it political instability and suffering (Acquaah–Gasie 2001:Online).

The 2014 PricewaterhouseCoopers Global Economic Crime Survey (2014:Online) indicated that 69% of South African respondents experienced fraud in 2012 and 2013 (37% globally) – an increase from 60% in 2009 (33% globally). In the 2013 Corruption Perception Index, the Republic of South Africa scored 42 on a scale of 0 to 100 (0 highly corrupt and 100 very clean). According to the index, 69% of the countries ranked below 50 revealed a serious fraud problem (Transparency International 2013:Online). Moreover, the Republic of South Africa was one of the four African countries that made up 74% of the fraud cases reported in Africa according to the KPMG Africa Fraud Barometer (2012:Online).

Given the current state of fraud, governments and corporates agree that fraud is bad for humanity and business, and action is required to mitigate this pandemic (Ernst & Young 2014:Online).

One of the challenges of fraud is that its impact is equivalent to that of a financial iceberg; some of the direct losses are plainly visible, while others are not easily detected and may include massive losses (Association of Certified Fraud Examiners 2014: Online). However, the level and impact of fraud can only be assessed based on known fraud (Carson, Verdu & Wokutch 2008). According to a KPMG survey (2013:Online), approximately 72% of uncovered fraud was perpetrated over a period of one to five years, which implies that fraud not reported timeously, the consequences may be unpleasant.

2 MEASURES TO CURB FRAUD

With the constantly changing nature of fraud, organisations need to be proactive in the identification of fraud and its perpetrators in order to enhance their anti-

fraud controls (KPMG 2013:Online). Whistleblowing as a measure to curb fraud will be the primary discussion in this article. However, a high-level overview of certain anti-fraud measures implemented in the public sector, such as, fraud risk management strategies, fraud risk assessments, and oversight bodies is also provided.

2.1 Fraud risk management strategies

Fraud risk management strategies (including fraud prevention plans) set the tone at the top, highlight an organisation's fraud tolerance level and set responsibilities for fraud prevention and anti-fraud controls. Section 38 of the Public Finance Management Act (29 of 1999), as amended, and regulation 3.2.2 of the Treasury Regulations issued in terms of the Public Finance Management Act require government departments to implement fraud prevention plans in the fight against fraud.

2.2 Fraud risk assessments

Risk assessment is "a systematic process adopted in order to quantify or qualify the level of risk associated with identified risks, to enrich the risk intelligence available to the institution" (Mafunisa 2014: 1240: Online). It also includes an element of fraud awareness which cautions employees to be on the look-out for fraud incidents - which also encourages whistleblowing. According to the Pricewaterhouse Coopers survey (2014:Online), fraud risk management including fraud risk assessment has proven to be an effective method to detect fraud in the Republic of South Africa (17%).

2.3 Other oversight/regulatory bodies

In the public sector, the Public Service Commission, Office of the Public Protector and the Auditor-General are three of the government oversight bodies that provide for initiatives that fight fraud. Public officials are required to report any fraudulent activities to these and other related authorities in terms of section 4.4.1 of the Code of Conduct for the Public Service.

2.4 Whistleblowing

In terms of section 2 of the Protected Disclosures Act, its objective is to offer protection from occupational detriment to employees making a protected disclosure, and also to promote a positive culture for whistleblowing. The Protected Disclosures Act sets certain requirements which have to be met before a disclosure may be protected. The requirements vary and depend on the recipient of disclosure. The focus of this research will be on Section 9(1)(b) which sets a strict requirement for protection.

The Companies Act (71 of 2008) of the Republic of South Africa governs a number of public and private entities and also addresses the importance of whistleblowing. Section 159 of the Companies Act stipulates persons entitled to make a disclosure, disclosure requirements, and whistleblower compensation. Section 159(5) of the Companies Act prescribes that those who blow the whistle should be entitled to compensation from another person only when they suffer any detriment, and direct or indirect threats caused by another as a result of their disclosure. However, the form of compensation is not defined (Botha & Van Heerden 2014:Online).

Defining disclosure/whistleblowing

In terms of section 1 of the Protected Disclosures Bill, a "disclosure means any disclosure of information regarding any conduct of an employer, or of an employee or of a worker of that employer, made by any employee or worker who has reason to believe that the information concerned shows or tends to show one or more of the following: criminal offences; failure to comply with certain legal obligations; miscarriages of justice; endangering of the health or safety of individuals; damage to the environment; and unfair discrimination".

Diale (2005:Online) describes whistleblowing as publicly raising an alarm on fraud committed privately – which is likely to raise possible hostility. Binikos (2008: Online) defines it as a form of pro-social behavior when an employee reports fraud for corrective action. According to Jubb (1999:Online), the elements of whistleblowing include the act of reporting, the potential/actual fraud, the organisation in question, the receiver of reported information, and the outcome or corrective action. Holtzhausen (2007:Online) concurs with Jubb that the concept of whistleblowing involves the presence of certain actions by individuals in a specific process. A whistleblower ('relator') is an individual who reports information relating to criminal, unlawful or irregular conduct (Bosch & Le Roux 2011: Online). It involves citizens, employees and managers/ directors – with the aim of terminating fraud (Holtzhausen 2007). A whistleblower can be anyone, including current and former employees of the company/organisation or agency defrauding the government, competitors, employees of the state or local government, subcontractors and corporations (Vandekerckhove 2011).

Statistics on whistleblowing

Different fraud-related surveys published by accounting firms include the 2009 and 2014 Global Economic Crime Survey by PricewaterhouseCoopers, the 13th Global Fraud Survey by Ernst & Young in 2014, and the Global Profiles of the Fraudster by KPMG in 2013.

The PricewaterhouseCoopers survey revealed (2014: Online) that globally, 5% of all surveyed frauds were reported through formal whistleblowing systems in 2013 – a 2% decrease from the 7% in 2009. In the Republic of South Africa, 6% of all surveyed fraud was detected through formal whistleblowing in 2013 (PricewaterhouseCoopers 2014:Online). The Ernst & Young survey (2014:Online) revealed that globally, 45% of the respondents did not have whistleblowing mechanisms available to them in terms of mitigating the risk of fraud. The report by KPMG (2013:Online) revealed that of the 41% surveyed cases of collusion detected globally, 22% were detected through anonymous tip-offs and 19% through formal whistleblowing.

Unlike the surveys conducted by the afore-mentioned accounting firms, the Association of Certified Fraud Examiner's Report to the Nations (2014:Online) was

limited to occupational fraud, which included asset misappropriation, corruption, and financial statement fraud. The collected data revealed that: (i) organisations with hotlines detected fraud 50% faster than those without them; (ii) tips were the most common and effective fraud detection method; (iii) over 40% of all fraud cases were detected by tips; and (iv) the rate of tips as a detection method was more than twice that compared to other detection methods. The term "tips" seems to include whistleblowing by internal as well as external parties, and include information received on a hotline. Furthermore, includes anonymous communications, as well as communications from parties whose identities are known to the organisation. (Association of Certified Fraud Examiner 2014:Online). Occupational fraud occurs when employees (including directors) defraud their employer/organisation using a variety of methods (Lord 2010:Online). In simple terms, this refers to fraud perpetrated internally. Tips are a form of whistleblowing systems.

The Association of Certified Fraud Examiner's Report to the Nations (2014:Online) further revealed that 49% of tips on occupational fraud were reported by employees, (the highest detection method) followed by customers at 21.6%. This suggests that where reporting systems are enhanced and used effectively, employees are more likely to report fraud.

The importance of whistleblowing

Researchers consider that there is no better source of good information than an organisation's employees (Association of Certified Fraud Examiners 2014: Online; Martin 2010:Online; Crook 2000:Online). The best way to harness this information is to establish good, confidential whistleblowing systems with the objective of preventing and detecting fraud in the workplace (Crook 2000:Online; Martin 2010:Online). Employees are seen to be in the best position to detect and report fraud, as they are close to business processes (Sinzdak 2008:Online). Fraud is like a cancer; most people know who has it, those likely to have it, and it has become common in society (Cascarino 2013). It is, therefore, no surprise that section 159 of the Companies Act requires certain companies to have confidential reporting structures.

Whistleblowing is seen as being one of the most effective and least expensive measures to protect organisations' resources (Dworkin 1997:Online). Lewis (2006:Online) stresses that whistleblowing is a good practice and the costs associated with implementation are insignificant. Whistleblowing promotes and enhances good corporate governance in organisations (Botha & Van Heerden 2014:Online; Maroun & Wainer 2013: Online). An organisation with a culture that encourages whistleblowing would serve as an indirect deterrent to fraud, as employees considering fraud will know that their acts can be reported (Dworkin 1997:Online).

Legal obligation to report fraud

There are various legal obligations imposed on public officials to report fraud. These include, amongst others:

- Sections 32(6), 32(7) and 102(2) of the Municipal Finance and Management Act (56 of 2003), which requires the Accounting Officer, Council and the board of directors of municipalities to report to the South African Police Services instances of fraud, theft, irregular expenditure and/or other losses that occurred in the municipality which constitute a criminal offence.
- Regulation 12(e) of the Public Service Regulations requires an employee to report to appropriate authorities any instances of fraud, corruption and other activities that are in contravention of any law of which they become aware of.
- Section 38(1)(g) of the PFMA states that the Accounting Officer is required to report in writing to the Treasury on any, irregular, wasteful and fruitless and unauthorised expenditure relating to the procurement of goods and services.
- Regulations 9.1.2, 12.5.1, 16A8.3(f) and 16A8.5, of the Treasury Regulations issued in terms of the PFMA impose a duty on specific public officials to report unauthorised, irregular or fruitless and wasteful expenditure to the relevant bodies, such as the Accounting Officer and the South African Police Services.
- Section 34 of the Prevention and Combatting of Corrupt Activities Act (12 of 2004), imposes a duty on persons in positions of authority to report instances of fraud, theft, forgery or extortion; or the production of a forged document involving an amount equal or exceeding R100 000 to the South African Police Services.

The objective of whistleblowing is to report fraud with the aim to seek corrective action. Researchers consider whistleblowing as an important tool in fighting fraud. However, given the extent of fraud and the rate of whistleblowing in the Republic of South Africa, one can, however, question whether the aforementioned anti-fraud initiatives are effective. Although a definite answer to this may require further research - one may surely consider other initiatives, such as whistleblower rewards. Though the mere existence of the above legal duties to report fraud does, however, raise other issues such as whether one should in the first place reward public officials who in any event have a legal duty to report fraud.

3 REWARDING WHISTLEBLOWERS

The objective of this section is to discuss the conceptual issues relating to rewarding whistleblowers for disclosed information. The section expounds upon the experiences of the United States of America through the False Claims Act, and also the United Kingdom. Lastly, the position in the Republic of South Africa is considered in order to establish what could potentially motivate South Africans to blow the whistle in the absence of rewards.

3.1 United States of America

Rewarding under the False Claims Act

Incentivising whistleblowers is common practice in the United States of America through the False Claims Act. It started in 1863 in response to contractors defrauding the federal government (Dworkin 2010; Schnell 2013: Online). The False Claims Act was revised in 1986 to

facilitate financially rewarding whistleblowers (relators) in a much simpler and generous fashion – resulting in whistleblowers reaping even more rewards (Dworkin 2010). Prior to its revision, the False Claims Act was amended unfavorably in 1943 by reducing the reward to whistleblowers and with the provision that *qui tam* actions already known by the government could not be filed (Vandekerckhove 2011). A *qui tam* action (whistleblowing under the False Claims Act) is when a private citizen files a false claim (blows the whistle) on behalf of themselves and the government of the United States of America (Devine & Maassarani 2011).

How it works

The False Claims Act is only applicable to cases where the government is a victim (Public Concern at Work 2007:Online). Once a *qui tam* action is filed, it should remain under seal for 60 days for the government (the United States of America's Department of Justice) to consider whether the case is worth pursuing and whether to join prosecution (Pacini, Qui & Sinason 2007:Online; Friedman 1997: Online). In cases where the government joins prosecution, the probability of success is commonly higher; however, government intervention is usually low (Yeoh 2014:Online).

When the *qui tam* action is under seal, the whistleblower cannot disclose having filed a case or reveal any of the evidence (Devine & Maassarani 2011).

Section 3730 "(d)"(2) of the False Claims Act stipulates the minimum and maximum percentages for whistleblower rewards – to be 15% to 30% of recovered monies. Where the Department of Justice does not join prosecution, the whistleblower may receive 25% to 30% of recoveries and 15% to 25% where the Department of Justice does join prosecution (Vandekerckhove 2011; Yeoh 2014: Online). The reward is made to the whistleblower by the court only when the case is successful and prosecuted (Young 2009:Online). Only the information reported is considered and not the motive for blowing the whistle (Masters 2008:Online; Fisher, Harshman, Gillespie, Leland & Yeager 2001:Online).

The False Claims Act is designed to meet the requirements that the reward is: (i) sufficiently "large" and "certain" to justify the whistleblower's effort; and (ii) timely in relation to doing the anticipated activity (Vandekerckhove 2011). Vandekerckhove (2011) further indicates that rewarding the whistleblower is different from purchasing information relating to fraud cases.

Additional reward

Section 3730 "(d)"(2) of the False Claims Act states that in addition to the reward, the whistleblower "shall also receive an amount for reasonable expenses which the court finds to have been necessarily incurred, plus reasonable attorneys' fees and costs".

Statistics of the False Claims Act

The recent largest healthcare fraud uncovered by the Department of Justice through the False Claims Act involved over 243 defendants in 17 federal districts – for false billings amounting to approximately USD$712 million (Department of Justice 2015: Online). This follows the False Claims Act recoveries of USD$5.69 billion in the 2014 fiscal year (Department of Justice 2014:Online). To further demonstrate its successes, there are the following False Claims Act statistics: approximately 647 *qui tam* actions were filed in 2012 compared to 35 filed in 1987 (Department of Justice 2012:Online); up to 4200 *qui tam* actions were pursued between 1987 and 2003, with up to USD$7.8 billion in recoveries (Pacini *et al* 2007:Online); between 2006 and 2007 over USD$1.45 billion was recovered by the USA Government in False Claims Act settlement judgments (Young 2009:Online); and in 2012, approximately USD$16 trillion in False Claims Act settlement judgments had been recovered. Approximately 16% was paid to whistleblowers (Rapp 2012:Online).

To help determine whether the False Claims Act route is worth considering in the Republic of South Africa, certain advantages and disadvantages of the False Claims Act experienced in the United States of America are now considered:

Benefits of the False Claims Act

Requires information from original source

- Section 3730(4A) of the False Claims Act states that the case must be filed by a person with an *original source* of information. Section 3730(4B) of the False Claims Act defines an *original source* as "*an individual who has direct and independent knowledge of the information on which the allegations are based and has voluntarily provided the information to the government before filing an False Claims Act action under this section which is based on the information*".
- The whistleblower needs to provide specific information such as what, why, and how, and therefore fabricating information may not be easy, thereby potentially limiting false allegations (Carson *et al* 2008).

Compensated for suffering

- Whistleblowers recover sufficient monies to withstand suffering from possible job loss, tarnished careers and retaliation (Dworkin 2010). In addition to protection afforded, monies paid to the whistleblower offset costs incurred (Carson *et al* 2008).

No success, no reward

- There is generally no reward for failed cases (Dworkin 1997:Online). For successful cases, the government will recover monies and tax payers will benefit (Carson *et al* 2008).

Supports informers and supplements with required resources

- Most complex cases are difficult to detect without inside information which can be successfully provided by inside informers (Bucy 2003:Online). The law facilitates the obtaining of information from informers in order to successfully prosecute cases (Pacini *et al* 2007:Online).

- The two successful features of *qui tam* as a tool of good external corporate governance and regulatory are: (i) the dissemination of information is facilitated by the law; and (ii) the law supplements limited resources of government attorneys and investigators (Pacini *et al* 2007: Online; Fisher *et al* 2007:Online). With its large recoveries, attorneys are prepared to undertake such cases (Dworkin 2010).

Statistics indicate the benefits outweigh the costs

- From 1997 to 2001 the costs for *qui tam* actions were USD$1.88 billion, whereas the benefits were USD$26.8 billion to USD$97.7 billion (Carson *et al* 2008).

- In its 2014 fiscal year, the United States of America recovered $5.69 billion through False Claims Act (Department of Justice 2014:Online).

Supports external reporting

- In cases where internal reporting options have been exhausted, external reporting is enabled, assisting whistleblowers to change things internally (Kesselheim 2010:Online).

- Moreover, Zhang, Chiu, and Wei (2009:Online) argued that where evidence is strong and an incentive is available, external reporting intentions are the strongest, however, such intentions decreased where evidence is weak.

Drawbacks of the False Claims Act

Time lag

- Although the general rule is 60 days for the government to consider whether to pursue a case (under seal), it is not uncommon that the government could take one to two years before deciding (Dworkin 2010). In worse cases, it may exceed five years (Devine & Maassarani 2011).

- The prosecution process under the False Claims Act may take long – ranging from two to five or more years (Devine & Maassarani 2011). Meanwhile, the burden of prosecution costs may be difficult for the whistleblower (Carson *et al* 2008). While waiting, the whistleblower may suffer from retaliation and alternative employment becomes difficult.

Morally/ethically questionable

- Certain questions raised about rewarding whistleblowers, include: (i) is rewarding the best way to curb fraud; and (ii) are "snitchers" desirable in the workplace? (Dworkin 1997:Online). Whistleblower rewards may possibly raise concerns on whether a moral atmosphere is desired within an organisation. Rossouw (2004) considers that adding an ethical dimension in the fight against fraud in an organisation can undermine the motivation and rationalization to commit fraud.

Potential conflict between the whistleblower and employer

- The False Claims Act requires external reporting – which is likely to raise conflict between the whistleblower and employer (Dworkin 1997: Online). Traditionally, whistleblowers are encouraged to firstly blow the whistle internally and only report externally when all internal systems are exhausted (Holtzhausen 2009:Online). Miceli, Near & Dworkin (2009:Online) assert that certain managers may be anxious with external reporting – because it may be viewed as being disloyal and undermining management authority.

No money recovered, no reward

- Fraud losses also include non-financial losses. With the False Claims Act, non-financial fraud losses equal no reward (Dworkin 1997:Online). It may, therefore, be argued that the reporting of matters which do not result in an identifiable financial loss is not as encouraged.

Pending cases and publicly known information

- Where a civil case is already pending and the government is party to the case, and the information disclosed is publicly available, the whistleblower may not file a *qui tam* action (Friedman 1997:Online). This is a pitfall where the plaintiff is willing to testify and has valuable information that may complete the case.

Delayed reporting

- It is argued that whistleblowers tend to delay reporting to allow the fraud to accrue more value to support higher rewards (Carson *et al* 2008). Unfortunately, the cost of silence on fraud is devastatingly high on human lives, employment, and lifelong savings (Auriacombe 2004:Online); and the longer the fraud goes undetected, the more financial damage is caused (Association of Certified Fraud Examiners 2014:Online).

Conclusion

The False Claims Act facilitates for financial rewards to whistleblowers who reported information on fraud perpetrated against the government of the United States of America. The False Claims Act was amended in 1986 to reward whistleblowers more generously. Since its amendment, the False Claims Act seems to be successful, with the government recovering lost monies and whistleblowers receiving lucrative rewards. Moreover, the government subsidies for the required resources and support informers, and attorneys are willing to take on *qui tam* actions.

Unarguably, the False Claims Act process may possibly be long, delayed, create conflict between employer and employee, result in no financial reward, expensive and morally questionable - which may add a great level of stress to the whistleblower. However, apart from its shortcomings which may have repercussions - the benefits of the False Claims Act appear to outweigh the costs associated with filing a *qui tam* action and yield great benefits for the United States of America.

3.2 United Kingdom

The United Kingdom's Public Interest Disclosures Act (Act of 2013) seeks to provide employees with protection against retaliation in the workplace as indicated in section 2 of the Public Interest Disclosures Act. It explicitly denies protection when whistleblowers do so for personal gain (Miceli *et al* 2009:Online) – unless otherwise provided under a statute including compensation for losses suffered (Public Concern At Work 2007:Online). The reason for not rewarding whistleblowers may derive from the belief that they should not be compensated (Bowden 2013:Online).

Rewarding whistleblowers

The concept of rewarding whistleblowers is not new in the United Kingdom. It begun in the 13th Century under a statutory scheme – until 1952 (Public Concern At Work 2007:Online). Young (2009:Online) posits that the introduction of *qui tam* actions was raised in the United Kingdom in 2007, but not pursued. Furthermore, in an attempt to discover how the United Kingdom Home Office would recover £250 million a year by 2010, the United Kingdom extensively debated rewarding whistleblowers with a percentage of the damages paid by the wrongdoer (Vandekerckhove 2011; Young 2009:Online). However, this initiative was not approved. Below, are some of the reasons for the rejection:

The United Kingdom's critics of the False Claims Act and rewarding of whistleblowers

Recently, the United Kingdom Financial Conduct Authority and Bank of England Prudential Regulation Authority rejected rewarding whistleblowers: and (i) argued that incentives in the United States of America do nothing for most whistleblowers, but only benefit a small number where reporting led to successful penalties imposed; (ii) maintained there is no empirical research indicating that incentivising whistleblowers would increase the rate of reporting or the quality thereof; and (iii) stressed they should rather encourage strengthening the current whistleblowing procedures and focus on its transparency (DiMauro 2014:Online).

Additional reasons for not adopting the reward principles include massive legal costs associated with the process; and complex and costly systems (Mont 2014:Online). This is further supported by research conducted by PricewaterhouseCoopers (2013:Online) in the United Kingdom. The research revealed that 52% of the organisations felt strongly that incentivising whistleblowers will not encourage an open culture of reporting (PricewaterhouseCoopers 2013:Online). The report further indicated that incentives require reporting to external regulators while on its own can lead to roguish acts, and the whistleblowers could potentially be the perpetrators (PricewaterhouseCoopers 2013:Online).

In the past, findings by the Public Concern At Work (2007:Online) on its quest to consider the False Claims Act provisions revealed that: (i) the successes of the False Claims Act in recovering defrauded government funds are acknowledged; (ii) the reward system offered in the United Kingdom from the 13th Century until 1951 was prone to abuse (e.g. wrongdoers defrauded the system in order to uncover minimal fraud); (iii) relying on the reward route has its difficulties as it is only after the fact, where the Public Interest Disclosures Act aims at preventing known fraud and fraud that is likely to happen; (iv) with the False Claims Act, expression of deterrence is outweighed by greed, where greed is used to suppress greed – which is regarded as dangerous, counter-productive and introducing more risks; (v) the United Kingdom encourages the reporting of fraud internally and acknowledge it to external regulators, although it is not the only way; and (vi) rewards undermine supportive cultural values.

For the above reasons the principles of the False Claims Act were not recommended in the United Kingdom. It was believed that measures such as the Public Interest Disclosures Act and adequate government contracts can serve the same purpose and also encourage reporting. The Public Concern At Work (2007:Online) concluded that False Claims Act recoveries seem to increase each year, implying that deterrence is outweighed by greed and such a provision is not recommended in the United Kingdom.

Response to critics

In response to some of the False Claims Act critics, Schnell (2013:Online) argues that: (i) the False Claims Act have been the linchpin to the United States of America's success in combating fraud against the government; (ii) it offers just and necessary incentives for the hardship experienced by whistleblowers in terms of physical, emotional and financial strain; (iii) there is no evidence that the False Claims Act has led to frivolous filing and waste of government resources; (iv) no evidence indicates that the False Claims Act encouraged external reporting compromising company internal reporting processes; and (v) reporting is not solely encouraged by financial reward, but also by citizens wanting to protect the public from harm – and therefore greed and self-centered individuals are not part of the equation.

Schnell (2013:Online) considers that the United Kingdom should look at adopting the False Claims Act in its attempt to enhance whistleblowing. However, this seems to have been dismissed by the United Kingdom given recent developments (DiMauro 2014:Online; Schnell 2014:Online). Schnell (2014: Online) further refers to the decision not to adopt whistleblower rewards by the United Kingdom as being a bad idea – especially in terms of overlooking the False Claims Act successes. The United Kingdom is still not convinced that this would work for them; however, the idea is not entirely dismissed (Schnell 2014:Online).

On the other hand, Bucy (2003:Online) considered that for an effective regulatory system, regulators should be willing to offer whistleblowers significant rewards for valuable information. In support, Dworkin (1997:Online) and Schnell (2013:Online) assert that a shift from the motivation of the whistleblower to the value of the information reported should be considered in the United Kingdom, in order to effectively encourage whistleblowing.

Conclusion
Whistleblower rewards are criticised in the United Kingdom. The Public Interest Disclosures Act focuses on whistleblower protection rather than whistleblower rewards. However, much as whistleblower rewards are criticised, the idea is not entirely rejected. The primary reasons for rejecting whistleblower rewards seem to be that focus should be on enhancing existing whistleblowing measures and that would serve the same purpose in encouraging whistleblowing. The Public Interest Disclosures Act and existing government contracts are considered to be effective as whistleblowing tools. However, researchers are still encouraging the United Kingdom to consider whistleblower rewards looking into the successes and benefits of the False Claims Act.

3.3 South Africa

Section 9(1)(b) of the Protected Disclosures Act and its application
Like most legislation, the Protected Disclosures Act is not free from criticism. This includes, amongst other things: (i) the limited definition of employee (Bosch & Le Roux 2011:Online); and (ii) not placing a legal duty on the employer to investigate and prosecute based on disclosed information (Diale & Holtzhausen 2005: Online). These and other concerns have been addressed in the Draft Protected Disclosures Bill, referred to *infra*.

However, the crux of this article is that section 9(1)(b) of the Protected Disclosures Act does not offer protection to employees who blow the whistle for personal gain, unless it is payable in terms of the law. Section 9 of the Protected Disclosures Act deals with the protection of whistleblowers who disclosed their concerns to persons or entities mentioned in section 8. If the information is disclosed in terms of this general disclosure for personal gain or to parties other than those mentioned in section 8 of the Protected Disclosures Act, the whistleblower will not be protected and his or her dismissal or occupational detriment will be lawful. The term "personal gain" is not defined in the Protected Disclosures Act and the question arises of what is the exact meaning of this term. In the *Tshishonga v Minister of Justice* matter it was held that incidental gains will not exclude protection.

From the aforesaid it is clear that an employer in the private sector may for instance internally reward its whistle-blowers and such a whistleblower will not forfeit protection solely because of that. This research, however, poses the question whether these types of initiatives should be applied in the Republic of South Africa and as such be regulated by legislation, such as the False Claims Act. If such legislation is passed, section 9 of the Protected Disclosures Act should, therefore, be reconsidered.

With the Protected Disclosures Act, whistleblower experience has been unpleasant in the Republic of South Africa. Numerous examples of this abound in popular media - but the matter of *Tshishonga v Minister of Justice*, is a striking example. In *Tshishonga's* matter the whistleblower was humiliated and suffered occupational detriment for reporting to the media; and was later dismissed (Le Roux 2010: Online). The court ruled that the disclosure was protected in terms of the Protected Disclosures Act but the whistleblower was only compensated with 12 month's remuneration for unfair dismissal (*Tshishonga v Minister of Justice* 2006:Online).

Another whistleblower was dismissed for reporting and was later compensated with six month's remuneration for unfair dismissal (*Magagane v MTN Group Management Services (Pty) Ltd* 2013:Online).

Both whistleblowers suffered occupational detriment for reporting. The form of compensation offered in these cases was for unfair dismissal suffered and not for reporting fraud. The compensation criteria for unfair dismissal are stipulated in sections 194(1) & 194(4) of the Labour Relations Act (12 of 2002), as amended, which is a separate issue from the rewards discussed in this article.

The challenge with the Protected Disclosures Act is that whistleblowers are only compensated for loss of salary or occupational detriments suffered as a result of reporting fraud and ultimately lose their jobs (Earle & Madek 2007:Online). Moreover, in their pursuit to fight fraud, their careers are tarnished and lives disturbed (Diale 2005:Online). Whistleblowing carries with it excessive emotional and psychological despair, and in the extreme, even the death of whistleblowers (Devine & Maassarani 2011; Tavakolian 1993: Online). The Protected Disclosures Bill partially addresses some of these issues as highlighted below. However, the primary focus of this article is to provide additional motivation to blow the whistle through financial rewards/incentives.

The Protected Disclosures Bill
To address its critics, the Protected Disclosures Act was amended in terms of section 7(1) of the South African Law Reform Commission Act (19 of 1973), as amended. Amendments included:

- Insertion of section 3A and 3B to address joint liability and duty to investigate. Section 3A places liability on the employer and other third parties subjecting an employee/worker to occupational detriment as a result of blowing the whistle. Section 3B further added an obligation for the employer to investigate and prosecute following a disclosure.
- Section 4 was amended with the insertion of section 1B indicating that where the court is satisfied that an employee/worker has suffered occupational detriment, the employer should make a payment to the employee/worker for any damages suffered by the employee/worker.
- Amendment to section 6 includes the employer's duty to have appropriate internal procedures for receiving and dealing with disclosed information, and informing every employee/worker about reporting procedures.

No amendments were included in the Bill with regard to section 9(1)(b) of the Protected Disclosures Act. In section 1B of the Protected Disclosures Bill, the employee/worker has to suffer some form of

occupational detriment and/or damages to qualify for any form of compensation. This article considers whistleblower reward regardless of occupational detriment or damages suffered.

Recent developments

Recently (Deputy Public Protector (PP) 2015), Advocate Malunga highlighted the need to incentivise whistleblowers in the Republic of South Africa. In his initiative, reference was made to the unpleasant incidences suffered by South African whistleblowers versus the successes of the False Claims Act (Nicolson 2015:Online). The view of incentivising whistleblowers is shared by Razzano (2014:Online) – who holds that the principles of the False Claims Act would assist in addressing the challenges of the Protected Disclosures Act regarding the lack of compensation. As Sehgal (2014) states, whistleblowers should not be treated like traitors, but celebrated and rewarded like heroes for doing the right thing.

Conclusion

In the Republic of South Africa, whistleblowers are only compensated for occupational detriment suffered and not for blowing the whistle as per the Protected Disclosures Act. The Protected Disclosures Bill only considers whistleblower compensation when the latter has suffered occupational detriment for reporting fraud. Protection is not afforded in cases where whistleblowers received a reward for reporting fraud unless it is payable in terms of the law.

However, despite the Protected Disclosures Act provisions, whistleblowers still suffer retaliation for blowing the whistle. The article considers that the Republic of South Africa should consider rewarding whistleblowers for reporting valuable information that led to prosecutions or the successful detection of fraud. Such compensation should be to compensate whistleblower travails.

4 DECISION TO BLOW THE WHISTLE

4.1 What motivates South Africans to blow the whistle?

In order to implement correct measures to encourage whistleblowing, it is crucial to understand the motivational factors which influence the decision to report fraud. According to studies in the Republic of South Africa, emphasis was placed on issues of integrity, trust in organisations, and good whistleblowing systems as motivational factors to whistleblowing.

In a study of organisations employing more than 50 employees in the Nelson Mandela Metropole, Perks and Smith (2008:Online) observed that whistleblowing can be improved by focusing on ethical issues and integrity in the workplace. Important issues for consideration included ethics' audits, clear whistleblowing policies, establishment of ethics committees, and ethics training (Perks & Smith 2008: Online). Acquaah-Gasie (2001:Online) states that employees are more likely to report fraud if they understand that by contributing to workplace integrity, they advance their wellbeing and that of their communities.

To encourage whistleblowing, Diale (2010:Online) suggests a whistleblower framework as advocacy for organisational integrity. This implies that whistleblowing should be properly and positively defined, interpreted, well-positioned, and considered a value add rather than a once-off activity (Diale 2010:Online). Auriacombe (2004:Online) stresses that it is key to design policies and procedures which positively encourage whistleblowing internally, by providing clear guidance on procedures to be followed by whistleblowers and managers in addressing reported matters. The emphasis is to ensure a culture of integrity – and then whistleblowing would follow. However, Holtzhausen (2007:Online) holds that one of the concerns of the Republic of South Africa is integrity in government and the implementation of measures that promote ethical reporting.

A study by Binikos (2008:Online) on a company operating in the Information and Communication Technology sector focused on the relationship between trust in the organisation and internal whistleblowing. It indicated that in an organisation where the level of trust is low, chances of internal whistleblowing would be low – and *vice-versa* (Binikos 2008:Online). Minnaar (2011:Online) also suggests that in transparent systems where trust exists within communities, citizens would feel free to report to authorities and would also be willing to provide more information without fear. It could be inferred that a high level of trust may result in a conflict of loyalties and in turn discourage any form of whistleblowing. Therefore, the relationship between organisational trust and whistleblowing can occasionally be contradictory.

4.2 Factors that could influence the decision to blow the whistle

It is important to look at factors that may potentially influence the decision to blow the whistle on fraud – which may include the following:

- South Africans come from an environment where whistleblowing is viewed in the same light as "informing". Informers and their activities were resented in communities (Minnaar 2011:Online). Moreover, informers are often classified as selfish, snitchers and those who "split" on their friends (Minnaar 2011:Online). One could ask whether historical associations prohibit whistleblowing in the Republic of South Africa or if it is lack of incentives.

- Negative experiences by whistleblowers with the whistleblower legislation may contribute negatively to whistleblowing. This includes the stressful experience faced by whistleblowers relating to the lack of professional counseling that may possibly be required by them (Tavakolian 1993:Online).

- Regardless of their great contributions, whistle-blowers are still perceived as being disloyal (Hoffman & McNulty 2011).

Yeoh's (2014:Online) empirical study revealed that employees would first weigh the financial and non-financial benefits before they can blow the whistle. Despite legislation to enhance whistleblowing, the decision to blow the whistle on one's boss or

colleague still remains a tough decision and may raise issues of contention, loyalty and morality (Auriacombe 2004:Online; Public Concern At Work, 2007:Online). It poses a great dilemma and is often associated with psychological and financial problems (DLA Piper 2013:Online). Moreover, it can compromise one's career, job and reputation (Lee & Kleiner 2011: Online).

The decision to remain silent may be influenced by several factors. According to Auriacombe (2004: Online), one of the results of a culture of silence is that society values compensation and punishment more than a culture of detection and deterrence of fraud. Thus it can be argued that in an organisational culture where compensation and punitive measures do not exist, the rate of whistleblowing may be very low or non-existent.

As indicated by several researchers above, an ethical organisational culture and integrity in the workplace is desirable to encourage whistleblowing. Employees are likely to behave according to set standards and values as well as disregard their own. Moreover, where employees perceive the level of ethical commitment by the employer to be stronger, the rate of reporting seems to be on the rise.

In the presence of all these measures, whistleblowing is on the decrease in the Republic of South Africa – could it be as a result of fear? Could whistleblower reward serve as a motivational factor for their efforts and bravery? A study to determine whether rewards could positively influence whistleblowing in the Republic of South Africa would be beneficial.

5 LIMITATIONS

An extensive literature review was conducted to address the research objective. The research was not a review of the affectivity of the legislative prescripts discussed or of the level of protection offered to whistleblowers in terms of relevant legislation. The research findings did not provide any assurance that the same False Claims Act benefits and drawbacks, as experienced in the United States of America, would be experienced in the Republic of South Africa – should similar provisions be considered. The research was limited to fraud perpetrated against the government. However, there is no restriction against a private sector entity rewarding persons who had blown the whistle against fraud.

6 OVERALL CONCLUSION

6.1 Recommendations and issues for consideration

The Republic of South Africa is a constitutional democracy and is governed by the rule of law. However, the rise of fraud has the potential to destroy the spirit of the new democracy. Thus there is a great need for courageous individuals to report fraud. Whistleblowing provides valuable service to organisations and the public. It is the most cost-efficient method to detect and promote good governance.

The United States of America, United Kingdom and the Republic of South Africa have implemented legislation in terms of whistleblowing to enhance good governance in the workplace. The False Claims Act in the United States of America and associated rewards appears to have proven successful withstanding its drawbacks. However, the United Kingdom still criticises whistleblower rewards and places reliance on the Protected Interest Disclosures Act and other government measures.

The Protected Disclosures Act in the Republic of South Africa on the other hand, denies whistleblowing for personal gain unless it is payable in terms of the law. However, the decision to blow the whistle is still a difficult one given the challenges whistleblowers face, specifically in the Republic of South Africa.

The article suggests that compensating whistleblowers in the fight against fraud be considered in the Republic of South Africa - considering the principles of the False Claims Act. Whistleblowers should not only be compensated for loss of pay or occupational detriment suffered, but be treated like the heroes they are and compensated for their efforts.

However, much as the benefits of the False Claims Act are attractive and yield great benefits for the United States of America, an empirical study should be conducted in the Republic of South Africa to determine whether rewarding whistleblowers would yield positive results should it be considered.

Rewarding whistleblowers would require amending section 9(1) (b) of the Protected Disclosures Act or introduction of a new law facilitating whistleblower rewards. When considering whistleblower rewards, the following may be considered:

- The False Claims Act benefits and drawbacks - and the False Claims Act critics in the United Kingdom.
- If personal gain for whistleblowing would benefit the economy of the Republic of South Africa and whether the country would morally justify financial incentives for doing the right thing.
- If rewarding public officials for reporting fraud can be justified since it forms part of their legal duties.
- The provision of temporary financial relief when cases take longer and where the whistleblower has been dismissed or suffering financial harm.
- The need for one dedicated body responsible for dealing with claims – to minimize delays and possible multiple reporting.

REFERENCES

Acquaah-Gasie, G. 2001. Fighting public officer and corporate crimes. *Transactions of the Centre for Business Law*, 33:88-104. SA ePublication. [Online]. http://www.0-reference.sabinet.co.za.innopac.up.ac.za/sa_epublications (Accessed: 01 June 2014).

Association of Certified Fraud Examiners. 2014. *Report to the nation on occupational fraud and abuse.* [Online]. http://www.acfe.com/rttn/docs/2014-report-to-nations.pdf (Accessed: 17 September 2014).

Auriacombe, C. 2004. Key issues in the whistle blowing process. *Journal of Public Administration*, 39(4):655-669. SA ePublications. [Online]. http://www.0-reference.sabinet.co.za.innopac.up.ac.za/sa_epublications (Accessed: 01 June 2014).

Binikos, E. 2008. Sounds of silence: Organisational trust and decisions to blow the whistle. *SA Journal of Industrial Psychology,* 34(3): 48-59. SA ePublications. [Online]. http://www.0-reference.sabinet.co.za.innopac.up.ac.za/document/EJC89161 (Accessed: 01 June 2014).

Bosch, C. & Le Roux, R. 2011. Not letting them whistle: The labour appeal court's approach to the Protected Disclosures Act and protecting parliament's employees. *Obiter*, 32(2):591-612. SA ePublications. [Online]. http://www.0-reference.sabinet.co.za.innopac.up.ac.za/sa_epublications (Accessed: 01 February 2014).

Botha, M.M. & Van Heerden, C.V. 2014. The Protected Disclosures Act 26 of 2000, the Companies Act 71 of 2008 and the Competition Act 89 of 1998 with regard to whistle-blowing protection: Is there a link? *Tydskrif vir die Suif-Afrikaanse Reg*, 2:337-358. SA ePublications. [Online]. http://www.0-reference.sabinet.co.za.innopac.up.ac.za/document/EJC152114 (Accessed: 24 May 2015).

Bowden, P. 2013. Whistleblowing needs a mother. *E-journal of International and Comparative Labour Studies*, 2(3):1-26. September-October. [Online]. http://www.adapt.it/EJCLS/index.php/ejcls_adapt/issue/view/12 (Accessed: 21 August 2014).

Bucy, P.H. 2003. Information as a commodity in the regulatory world. Available from: *Houston Law Review*, 3:905-978. [Online]. http://www.houstonlawreview.org/archive/downloads/39-4_pdf/Bucy.pdf (Accessed: 08 October 2014).

Carson, T.L., Verdu, M.E. & Wokutch, R.E. 2008. Whistle-blowing for profit: An ethical analysis of the Federal False Claims Act. *Journal of Business Ethics*, 77:361-376.

Cascarino, R.E. 2013. *Corporate fraud and internal controls*. New Jersey: John Wiley & Sons.

Crook, D. 2000. How to encourage whistleblowing. *Journal of Financial Regulation and Compliance*, 8(4):322-332. Emerald. [Online]. http://www.0-www.emeraldinsight.com.innopac.up.ac.za/doi/pdfplus/10.1108/eb025053 (Accessed: 01 February 2014).

Devine, T. & Maassarani, T.F. 2011. *A handbook for committing the truth: The corporate whistleblower's survival guide*. San Francisco: Berrett-Koehler Publishers, Inc.

Diale, A.J. & Holtzhausen, N. 2005. Public or protected disclosure? The fallacy of whistleblower protection in South Africa. *Journal of Public Administration*, October: 10–19. SA ePublications. [Online]. http://www.0-reference.sabinet.co.za.innopac.up.ac.za/document/EJC51233 (Accessed: 1 February 2014).

Diale, A.J. 2005. Swimming against the tide: The plight of a whistleblower in South Africa. *Journal of Public Administration*, 40(3.1):269-279. SA ePublications. [Online]. http://www.0-reference.sabinet.co.za.innopac.up.ac.za/webx/access/electronic_ _journals/jpad/jpad_v40_n3_si1_a8.pdf (Accessed: 01 February 2014).

Diale, A.J. 2010. The role and importance of whistle-blowing in building organisational integrity in the public sector: A theoretical exposition. *Journal of Public Administration,* 45(1.1):295-305. SA ePublications. [Online]. http://www.0-reference.sabinet.co.za.innopac.up.ac.za/sa_epublications (Accessed: 01 June 2014).

DiMauro, J. 2014. UK says 'no thanks' to U.S. style whistleblower rewards. *The FCPA* Blog, 31 July 2014. [Online]. http://www.fcpablog.com/blog/2014/7/31/uksaysnothankstousstylewhistleblowerrewards.html# (Accessed: 19 February 2015).

DLA Piper. 2013. *Whistleblowing: An employer's guide to global compliance*. [n.p.] 2669827. [Online]. http://www.dlapiperuknow.com/export/sites/uknow/products/files/uknow/DLA-Piper-Whistleblowing-Report.pdf (Accessed: 14 October 2014).

Dworkin, T.M. 1997. Whistleblowing: Should greed be the goad for good? *Journal of Financial Crime*, 4(4):336-342. Emerald. [Online]. http://www.dx.doi.org/10.1108/eb025800 (Accessed: 11 September 2014).

Dworkin, T.M. 2010. US Whistleblowing: a decade of progress? In: Lewis, D. (ed.), *A global approach to public disclosure – What can we learn from existing whistleblowing legislation and research?* Glos, UK: Edward Elgar Publishing Ltd:36-55.

Earle, B.H. & Madek, G.A. 2007. The mirage of whistleblower protection under Sarbanes-Oxley: A proposal for change. *American Business Law Journal*, 44(1):1-54. EBSCOhost. [Online]. http://www.0-web.a.ebscohost.com.innopac.up.ac.za/ehost/pdfviewer/pdfviewer?vid=5&sid=90a30909-3a02-49ab-9c53-97084f7415b8%40sessionmgr4003&hid=4114 (Accessed: 08 February 2014).

Ernst & Young. 2014. *Overcoming compliance fatigue - Reinforcing the commitment to ethical growth: 13th Global Fraud Survey*. [Online]. http://www.ey.com/Publication (Accessed: 28 September 2014).

Fisher, J., Harshman, E., Gillespie, W., Leland, O. & Yeager, F. 2001. Privatising regulation: Whistleblowing and bounty hunting in the financial services industries. *Journal of Financial Crime*, 8(4):305-318. Emerald. [Online]. http://www.dx.doi.org/10.1108/eb025995 (Accessed: 12 July 2015).

Friedman, D.S. 1997. USA: Private prosecution of criminal conduct. *Journal of Financial Crime*, 5(2):130-137. Emerald. [Online]. http://www.dx.doi.org/10.1108/eb025825 (Accessed: 11 September 2014).

Hoffman, W.M. & McNulty R.E. 2011. A business ethics theory of whistleblowing: Responding to the $1 trillion question. In: Arszutowicz, M. & Gasparski, W.W. (ed.). *Whistleblowing in defense of proper action: Praxiology: The International Annual of Practical Philosophy and Methodology*. New Brunswick, N.J.: Transaction Publishers:45-59.

Holtzhausen, N. 2007. Whistleblowing for good governance: Issues for consideration. *Journal of Public Administration,* 42(5):46-58. SA ePublications. [Online]. http://www.0-reference.sabinet.co.za.innopac.up.ac.za/webx/access/electronic _journals/jpad/jpad_v42_n5_a6.pdf (Accessed: 01 February 2014).

Holtzhausen, N. 2009. Organisational trust as a prerequisite for whistleblowing. *Journal of Public Administration*, 44(1.1):234-246. SA ePublications.[]. [Online]. http://www.0-reference.sabinet.co.za.innopac.up.ac.za/webx/access/electronic _journals/jpad/jpad_v44_n1_si1_a13.pdf (Accessed: 01 February 2014).

Jubb, P.B. 1999. Whistleblowing: A restrictive definition and interpretation. *Journal of Business Ethics*, 21(1):77-94. Available from: ProQuest Business Collection: [Online].http://www.search.proquest.com.innopac.up.ac.za/docview/198112534/fulltextPDF/E3832EC1A8204A07PQ/7?accountid=14717 (Accessed: 09 January 2014).

Kesselheim, A.S. 2010, Whistle-Blowers' Experiences in Fraud Litigation against Pharmaceutical Companies. *The New England Journal of Medicine*, 362 (19):1832-1839. [Online]. http://www.nejm.org/doi/pdf/10.1056/NEJMsr0912039> (Accessed: 16 November 2014).

KPMG. 2012. Africa Fraud Barometer – Assess your risk before doing business in Africa. [Online]. http://www.kpmg.com/Africa/en/IssuesAndInsights/Articles-Publications/Press-Releases/Documents/Africa (Accessed: 17 October 2016).

KPMG. 2013. Global profiles of the fraudster white-collar crime – present and future. [Online]. http://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/ (Accessed: 28 September 2014).

Le Roux, R. 2010. The Protected Disclosures Act 26 of 2000: is this as good as it is going to get for whistleblowers? A review of some recent jurisprudence. *Stellenbosch Law Review*, 21(3):508-527. SA ePublications. [Online]. http://www.0-reference.sabinet.co.za.innopac.up.ac.za/document/EJC54754 (Accessed: 01 February 2014).

Lee, K. & Kleiner, B. 2011. Whistleblower retaliation in the public sector. *Public Personnel Management*, 40(4): 341-348. EBSCOhost. Business Source Premier. [Online]. http://www.0-web.b.ebscohost.com.innopac.up.ac.za/ehost (Accessed: 08 February 2014).

Lewis, D. 2006. The contents of whistleblowing/confidential reporting procedures in the UK: Some lessons from empirical research. *Employee Relations*, 28(1):76-86. Emerald. [Online]. http://www.dx.doi.org/10.1108/01425450610633073 (Accessed: 01 October 2014).

Lord, A.T. 2010. The prevalence of fraud: What should we, as academics, be doing to address the problem? *Accounting and Management Information Systems*, 9(1):4-21. Proquest. [Online]. http://www.0-search.proquest.com.innopac.up.ac.za/docview/853704540/fulltextPDF/26765DD4A36C418APQ/8?accountid=14717 (Accessed: 26 October 2014).

Mafunisa, M.J. 2014. Preventing corruption in the South African public service: The case of fraud prevention plans. *Journal of Public Administration*, 49(4):1230-1243. SA ePublication. [Online]. http://www.0-reference.sabinet.co.za.innopac.up.ac.za/webx/access/electronic_journals/jpad/jpad_v49_n4_a19.pdf (Accessed: 29 July 2015).

Maroun, W. & Wainer, H. 2013. To report or not to report: In what context is a "reportable irregularity" reportable? *South African Journal of Economic and Management Sciences*, 16(1):13-25. SA ePublications. [Online]. http://www.0-reference.sabinet.co.za.innopac.up.ac.za/sa_epublications (Accessed: 01 June 2014).

Martin, P. 2010. *The state of whistleblowing in South Africa: taking stock*. [Online] https://www.openjournalismworkshop.files.wordpress.com/2013/03/odac_whistleblowing_report_web.pdf (Accessed: 17 August 2015).

Masters, J.L. 2008. Fraud and money laundering: The evolving criminalisation of corporate non-compliance. *Journal of Money Laundering Control*, 11(2):103-122. Emerald. [Online]. http://www.0-www.emeraldinsight.com.innopac.up.ac.za/doi/pdfplus/10.1108/13685200810867447 (Accessed: 11 September 2014).

Miceli, M.P., Near, J.P. & Dworkin, T.M. 2009. A word to the wise: How managers and policy-makers can encourage employees to report wrongdoing. *Journal of Business Ethics*, 86:379-396. Available from: Google Scholar: [Online]. http://www.download.springer.com/static/pdf/224/art%253A10.1007%252Fs10551-6.pdf?auth66=1421042951_66a7f9470916880266e6c1413dba875a&ext=.pdf (Accessed: 12 January 2015).

Minnaar, A. 2011. The use of informers: An essential tool in the fight against crime? *Southern African Journal of Criminology*, 24(3):83-97. SA ePublications. [Online]. http://0-reference.sabinet.co.za.innopac.up.ac.za/sa_epublications (Accessed: 01 June 2014).

Mont, G. 2014. Top UK regulators reject whistleblower rewards. *Compliance Week, 31 July 2014.* [Online]. http://www.complianceweek.com/blogs/the-filing-cabinet-global-glimpses-enforcement-action/top-uk-regulators-reject-whistleblower#.VOY1fvmUfkU (Accessed: 19 February 2015).

Nicolson, G. 2015. Time to sweeten the deal for whistleblowers? D*aily Maverick*, 30 January 2015. [Online]. http://www.dailymaverick.co.za/article/2015-01-30-time-to-sweeten-the-deal-for-whistleblowers/#.VN9w4vmUfkU (Accessed: 14 February 2015).

Pacini, C. Qui, L.H. & Sinason, D. 2007. Qui tam actions: fighting fraud against the government. *Journal of Financial Crime*, 14(1):64-78. Emerald. [Online]. http://www.emeraldinsight.com.innopac.up.ac.za/doi/pdfplus/10.1108/13590790710721819 (Accessed: 01 February 2014).

Perks, S. & Smith, E. 2008. Employee perceptions regarding whistle-blowing in the workplace: a South African perspective. *SA Journal of Human Resource Management*, 6(2):15-24. SA ePublications. [Online]. http://www.0-reference.sabinet.co.za.innopac.up.ac.za/document/EJC95873 (Accessed: 01 June 2014).

PricewaterhouseCoopers. 2013. *Striking a balance: Whistleblowing arrangements as part of a speak up strategy*. [Online]. http://www.pwc.co.uk/fraud-academy/publications/whistleblowing-striking-a-balance.jhtml (Accessed: 19 February 2015).

PricewaterhouseCoopers. 2014. *Global economic crime survey*. [Online]. http://www.pwc.com/crimesurvey (Accessed: 21 February 2014).

Public Concern at Work. 2007. Rewarding whistle-blowers as good citizens: Response to the Home Office consultation. Public Concern at Work. [Online]. http://www.pcaw.org.uk/files/rewardingwhistleblowers-2008.pdf (Accessed: 08 October 2014).

Rapp, G.C. 2012. Mutiny by the bounties? The attempt to reform Wall Street by the new whistleblower provisions of the Dodd-Frank Act. BYU Law Review, 2012 1(2). [Online]. http://www.digitalcommons.law.byu.edu/cgi/viewcontent.cgi?article=2637&context=lawreview (Accessed: 17 August 2015).

Razzano, G. 2014. *Empowering our whistleblowers*. [Online]. http://www.r2k.org.za/wp-content/uploads/WhistleblowingBook.pdf (Accessed: 14 February 2015).

Republic of South Africa. 2006. *M.M. Tshishonga v The Minister of Justice and Constitutional Development and The Director General of the Department of Justice and Constitutional Development*. The Department of Justice. [Online]. http://www.doj.gov.za (Accessed: 02 February 2014).

Republic of South Africa. 2013. *Magagane v MTN SA (Pty) Ltd and MTN Group Management Services (Pty) Ltd*. The Department of Justice. Available from: http://www.doj.gov.za (Accessed: 1 June 2014).

Republic of South Africa. Code of Conduct for the Public Service. 2002. Public Service Commission.

Republic of South Africa. Companies Act, 71 of 2008. Pretoria: Government Printer.

Republic of South Africa. Labour Relations Act, 12 of 2002 (as amended). Pretoria: Government Printer.

Republic of South Africa. Municipal Finance and Management Act, 56 of 2003. Pretoria: Government Printer.

Republic of South Africa. Prevention and Combatting of Corrupt Activities Act, 12 of 2004. Pretoria: Government Printer.

Republic of South Africa. Protected Disclosures Act, 26 of 2000. Pretoria: Government Printer.

Republic of South Africa. Protected Disclosures Amendment Bill, 2014. Pretoria: Government Printer.

Republic of South Africa. Public Finance Management Act, 29 of 1999 (as amended). Pretoria: Government Printer.

Republic of South Africa. Public Service Regulations. 2015. Department of Public Service and Administration. Pretoria: Government Printer.

Republic of South Africa. South African Law Reform Commission Act, 19 of 1973 (as amended). Pretoria: Government Printer.

Republic of South Africa. South African Law Reform Commission. 2007. Report on Public disclosures. [Online]. http://www.justice.gov.za/salrc/reports/r_pr123_protected-disclosures_2007.pdf (Accessed: 02 March 2014).

Republic of South Africa. The Office of the Public Protector, 29 January 2015. Deputy Public Protector Advocate Kevin Malunga joins calls for whistleblowers to be incentivised. [Online]. http://www.gov.za/deputy-public-protector-joins-calls-whistleblowers-be-incentivised (Accessed: 2 February 2015).

Republic of South Africa. Treasury Regulations for departments, constitutional institutions and public entities. Issued in terms of the Public Finance Management Act, 1999. Pretoria: Government Printer.

Rossouw, D. 2004. *Business ethics*. 3rd ed. South Africa: Oxford University Press.

Schnell, G. 2013. Message to the UK – Whistleblower incentives work. *Constantine Cannon, Whistleblower Practice*, 7 November 2013. [Online]. http://www.whistleblower-insider.com/message-uk-whistleblower-incentives-work/#.VOYzlfmUfkU (Accessed: 19 February 2015).

Schnell, G. 2014. UK rejects whistleblower rewards; at least for now. *Constantine Cannon, Whistleblower Practice, 26 June 2014.* [Online]. http://www.whistleblower-insider.com/uk-rejects-whistleblower-rewards-least-now/#.VOYxwfmUfkU (Accessed: 19 February 2015).

Sehgal, P. 2014. Whistleblowers: Traitors or heroes? A global perspective. Paper presented at Proceedings of 26th International Business Research Conference, 7-8 April 2014, London, UK: Imperial College:1-12.

Sinzdak, G. 2008. An analysis of current whistleblower laws: Defending a more flexible approach to reporting requirements. *California Law Review*, 96(6):1638-1668. Available from: EBSCOhost. Business Source Premier. [Online]. http://www.0-web.b.ebscohost.com.innopac.up.ac.za/ehost (Accessed: 08 February 2014).

Tavakolian, H.R. 1993. The perils of whistle blowing. *Management Research News,* 16(8): 1-5. Emerald. [Online]. http://www.dx.doi.org/10.1108/eb028324 (Accessed: 20 June 2015).

Transparency International. 2013. *Corruption Perceptions Index.* [Online]. http://www.transparency.org/whatwedo/publication/cpi_2013 (Accessed: 25 May 2015).

United Kingdom. Public Interest Disclosure Act, 2013.

United States of America. Department of Justice. 2012. *Statistics on FCA cases from 1986 through FY 2012.* Fraud statistics - overview. US: Civil Division. [Online]. http://www.sidley.com/files/upload/C-FRAUDS_FCA_Statistics%20pdf.pdf (Accessed: 24 September 2014).

United States of America. Department of Justice. 2014. *Justice Department recovers nearly $6 billion from false claims act cases in fiscal year 2014*. [Online]. http://www.justice.gov/opa/pr/justice-department-recovers-nearly-6-billion-false-claims-act-cases-fiscal-year-2014 (Accessed: 25 May 2015).

United States of America. Department of Justice. 2015. *National medicare fraud takedown results in charges against 243 individuals for approximately $712 million in false billing.* Justice News. [Online]. http://www.justice.gov/opa/pr/national-medicare-fraud-takedown-results-charges-against-243-individuals-approximately-712 (Accessed: 12 July 2015).

United States of America. Federal False Claims Amendments Act of 1986.

Vandekerckhove, W. 2011. Rewarding the whistleblower – disgrace, recognition, or efficiency? In: Arszutowicz, M. & Gasparski, W.W. (eds), *Whistleblowing in defense of proper action, Praxiology: The international Annual of Practical Philosophy and Methodology*. New Brunswick, N.J.: Transaction Publishers:21-31.

Yeoh, P. 2014. Whistleblowing: motivations, corporate self-regulation, and the law. *International Journal of Law and Management*, 56(6):1-16. Emerald. [Online]. http://dx.doi.org/10.1108/IJLMA-06-2013-0027 (Accessed: 01 October 2014).

Young, S.N.M. 2009. Why civil action against corruption? *Journal of Financial Crime*, 16(2):144-159. Emerald. [Online]. http://www.dx.doi.org/10.1108/13590790910951821 (Accessed: 11 September 2014).

Zhang, J. Chiu, R. & Wei, L. 2009. On whistleblowing judgment and intention: The roles of positive mood and organisational ethical culture. *Journal of Managerial Psychology*, 24(7):627-649. Emerald. [Online]. http://dx.doi.org/10.1108/02683940910989020 (Accessed: 01 October 2014).

The development of an integrated IT risk assessment questionnaire for internal auditors' use

R Goosen

School of Accountancy
Stellenbosch University

ABSTRACT

Most businesses today operate in a complex Information Technology (IT) environment. The King III Report, South Africa's Corporate Governance Framework, holds the board of directors responsible for risk management processes, including IT governance related matters. This responsibility is often delegated to the IT- and risk committees, which in turn are assessed and evaluated by the internal auditor. However, due to ever-changing emerging technology risks and the vague guidance provided by the King III Report, the internal auditor requires assistance to conduct this evaluation. Most of the frameworks recommended by King III Report have only been updated in recent years, thereby changing the focus and risk areas internal auditors should evaluate. This article proposes to develop an integrated IT risk assessment questionnaire based on certain updated IT and risk control frameworks to assist the internal auditor in evaluating high level IT control risk areas in an effective manner, whilst complying with the latest framework requirements and also taking emerging technology risks into consideration.

Key words

IT Audit; COSO; ERM; COBIT 5; ITIL V3; ISO 27001; ISA 27002; ISA 315; ISA 330; IT Risks

1 INTRODUCTION

1.1 Background

The IT-related risks of a company have significantly increased due to operating in an open, interconnected network, where users are able to gain access and transfer data to systems through mobile devices and cloud services (Huawei 2013:Online). In a recent survey, cyber security and data privacy were identified as the two biggest IT risk areas for companies (ISACA & Protiviti 2014:Online). The King III Report holds the board of directors ultimately responsible for risk management and IT governance related matters, whilst the internal auditor is often responsible to assess and evaluate the work of the IT and risk committees (IODSA 2009:82); Institute of Internal Auditors (IIA) 2009:4). However, King III Report refers briefly to certain IT and risk control frameworks which could be consulted. However, no specific detailed guidance is provided to assist the internal auditor in this regard (IODSA 2009:16). With the inclusion of emerging technologies such as mobile applications and cloud computing activities in the daily operations, the internal auditor recognizes the need to keep informed with these additional IT risks but finds it challenging to do so (Protiviti 2014: Online). They also need to keep up-to-date with the recently updated international control frameworks, including the new Committee of Sponsoring Organisations (COSO) framework, which forms the basis of most risk management processes, changing the scope and focus of the internal audit function significantly to include the risks emerging technologies pose to a company (Protiviti 2014:Online). This article will develop an integrated IT risk assessment questionnaire (hereafter referred to as 'the questionnaire'), based on the high level IT controls suggested by the COSO framework (COSO 2013), the Enterprise Risk Management (ERM) standard (COSO 2013; Curtis & Carey 2012:Online), The Control Objectives for Information and related Technology Framework, known as COBIT 5, (ISACA 2012:Online), The Information Technology Infrastructure Library Framework, known as ITIL v3, (Cartlidge, Rudd, Smith, Wigzel, Rance, Shaw & Wright 2011:Online) and The Code of Practice for Information Security Management standards, known as the ISO 27001 and 27002 standards (ISO 27002 2013).

This questionnaire, as developed in this article, is based on the latest versions of these control frameworks, which will assist the internal auditor to evaluate the effectiveness of the implemented key high-level IT controls including emerging technology risks, which could affect financial, operational and compliance concerns (IODSA 2009:16). The questionnaire is categorized in specific key IT risk control areas, either to be performed annually or regularly, to ensure that the relevant high level key IT risk areas have been considered and evaluated.

1.2 Historical research

Research on the implementation of an effective IT risk assessment has been addressed by various institutions.

In 2005, a practice guide was developed on how to implement a successful IT governance structure (NCC 2005:Online). The Information Technology Governance Institute (ITGI) conducted a mapping of the following processes: COBIT 4.1, ITIL and the ISO 27002 standard, which revealed how these frameworks' diverse focus areas may be used together to comply with IT governance requirements (ITGI 2008:Online). This article emphasized the importance of using COBIT as a basis for implementing IT controls in an IT environment, in combination with other control models (ITGI 2008:Online). Liell-Cock, Graham and Hill (2009:Online) discussed the alignment between IT governance and the King III Report whilst in 2010, Gheorghe proposed a high level IT assessment methodology through the use of ISACA's IT audit standards, COBIT 4.1, COSO, ITIIL, ISO 27002 and ISO 38500 (Gheorghe 2010:32-42). However, no reference is made to the importance of configuration controls in this article. Hardy (2006:55-61) and Steenkamp (2011:1-8) confirmed that by implementing the COBIT control framework, a company will comply with King III's IT governance requirements. However, all of the abovementioned research has since become outdated because the ITIL framework was updated in 2011 to provide clarity on IT service management matters (Cartlidge *et al* 2011:Online). The COBIT framework was also updated in 2012 (ISACA 2012:Online) as well as the COSO framework, which emphasized the importance of IT and enterprise risk management controls (COSO 2013).

A high level mapping between the latest ITIL framework and other IT control frameworks such as COBIT 4.1 and ISO 27002 was conducted by Ali, Soomro and Brohi (2013:1190-1196). A business continuity framework was developed by Svata (2013:19-35) through the utilisation of different risk management frameworks. However, this article only focussed on the business continuity aspects. Elhasnaoui, Medromi, Faris, Iguer and Sayouti (2014:157-161) proposed an IT governance architecture process based on the COBIT 5, ITIL V3 and ISO 27002 frameworks. The abovementioned articles only contained high-level mappings, which are of no practical use to the internal auditor. A mapping between COSO 2013 and COBIT 5 was conducted by ISACA, but it excluded other important frameworks (ISACA 2014:Online). Galligan and Rau (2015: Online) further discussed the importance of using the updated COSO framework to address cyber risks in an organization. The articles written by ISACA (2014:Online) and Galligan and Rau (2015:Online) did however, exclude other important frameworks as part of their findings.

Moreover, in the abovementioned research, limited attention was given to the importance of the configuration controls, which is critical in today's open-network environments, specifically relating to emerging technologies (Santarcangelo 2010:Online). These technologies could have a significant impact on the internal auditor's risk assessment process (Ernst & Young 2013:Online). Whilst valuable research has been conducted, its effective and practical application for internal auditors has been limited due to the theoretical nature of these discussions, which contain vast amounts of information without practical implementation guidance. It also discusses only certain aspects of the internal IT risk assessment process and does not address these at an integrated level.

1.3 Structure of the article

This article consists of the following sections: Section 2 contains the research objective and motivation. Section 3 contains the research methodology. Section 4 includes a literature review of the different control frameworks considered in developing the questionnaire. Section 5 presents the questionnaire, which could assist internal auditors to assess the IT risk environment effectively. An overview of the conducted research is summarised in section 6.

2 RESEARCH OBJECTIVE AND MOTIVATION

The internal auditor often needs to assess the risk management processes, including the IT risks in an IT environment, with reference to these articles (Basti 2015:Online; IIA 2009:Online; IODSA 2009:95). However, in the last few years, many well-known frameworks used by internal auditors have been updated and revised significantly, thereby changing the focus and areas of concern to also include the consideration of emerging technology risks as well as becoming more prevalent in the day-to day operations (COSO 2013; ISACA 2012:Online; ISO 27002 2013; Crown 2011).

The objective of this study is to develop an integrated IT risk assessment questionnaire, which can assist the internal auditor to assess and evaluate the key high level IT controls implemented by the risk and IT management teams. This would ensure that an effective evaluation is conducted, including the evaluation of emerging technology risks based on the latest control framework requirements.

The updated control frameworks mentioned below were researched to identify key high-level IT control risk areas, which need to be assessed by the internal auditor in an effective manner. It will assist internal auditors to acquire a greater understanding of the modern day IT environment, whilst posing the right type of questions. Value is also added by identifying controls which are lacking but should in fact be implemented.

The following internationally recognised control frameworks, based on IT and risk experts' knowledge, were used to develop the questionnaire for the following reasons: The COSO and ERM frameworks (COSO 2013:Online) were used to form the basis for risk management related matters. COBIT 5, a widely used IT control framework, provides guidance to identify high-level IT control processes but does not focus on the technical details (ISACA 2012) which will be provided by the frameworks mentioned below. ITIL v3 (Cartlidge *et al* 2011) discuss service management controls whilst the ISO 27001 and ISO 27002 standards (ISO 27002 2013; Praxiom 2013a:Online) focus on information security matters.

The questionnaire was developed by identifying and combining these high-level key IT risk areas from the

abovementioned frameworks, thereby providing the internal auditor with a condensed, integrated and combined version (or reference guide) to perform key IT risk assessment procedures effectively in a modern day environment, rather than consulting each individual framework separately, which contains detail and repetitive processes.

3 RESEARCH METHODOLOGY

The following approach was followed to develop the questionnaire:

i) The King III Report was researched to identify the roles and responsibilities assigned to the board of directors and the risk management and internal audit teams, with specific reference to IT governance matters and how to address IT risks in an IT environment (IODSA 2009:82,87).
ii) Research was conducted on the updated framework versions of COBIT 5 (ISACA 2012), ITIL V3 (Cartlidge *et al* 2011), ISO 27001 and 27002 (ISO 27002 2013; Praxiom 2013a & b) as well as COSO (COSO 2013) and the enterprise risk management processes (Curtis & Carrey 2012:Online).
iii) Key high level IT risk control areas were identified, summarized and categorized from these control frameworks and the results were presented as a questionnaire, which could assist internal auditors in asking the correct type of questions. The relevant high level key IT risk areas were considered and evaluated.

The study included academic research, working papers, peer reviewed journals as well as popular online articles.

4 LITERATURE REVIEW

In order to develop a questionnaire, research was conducted of the board of director's roles and responsibilities, risk management and internal audit teams as well as the relevant updated control frameworks and processes discussed below:

4.1 Planning an internal IT risk assessment

According to the King III Report, the board of directors are, *inter alia,* responsible for IT governance matters. This responsibility is often delegated to the risk and audit committees (IODSA 2009:87). The risk committee is responsible for developing, identifying and addressing enterprise-wide risks, including those specifically relating to IT matters (Broadleaf 2014: Online), whilst the internal auditors' duties involve evaluating the efficiency of implemented risk management processes (Broadleaf 2014:Online; IIA 2009). The role of the internal auditor is important to provide the board of director's independent assurance surrounding the reliability and appropriate assessment of these risks (IIA 2009). The more complicated the IT systems become, the more knowledge and skills the internal auditor needs in order to perform an effective assessment (Protiviti 2014:Online). In order to ensure that the relevant high level key IT risks are assessed by the internal auditor, the King III Report recommends that the relevant risk- and IT control frameworks are consulted to perform an effective internal IT risk assessment (IODSA 2009:16). The use of the questionnaire developed in this article is, therefore, based on these internationally recognised and widely used frameworks to identify key IT control areas which the internal auditor needs to consider during its IT risk assessment process. This will ensure that the questionnaire is based on an independent experts' knowledge base to assess the IT control environment.

4.2 Risk and IT control frameworks

The following internationally recognised and updated risk and IT control frameworks were researched in the development of the questionnaire:

4.2.1 COSO and ERM frameworks:

The COSO framework often forms the basis of designing and evaluating internal control processes. It assists in evaluating Enterprise Risk Management (ERM) processes and detecting fraudulent activities (COSO 2013). It also addresses the financial, operational, and compliance reporting controls, which need to be assessed by the internal auditor (IODSA 2009:93). This framework was updated in 2013 because companies placed greater emphasis on governance matters and the need for more risk assessment guidance on emerging technologies (COSO 2013; Protiviti 2013:Online).

The ERM framework, used complimentary to the COSO framework, provides guidance in establishing a risk management system by aligning the risk appetite and risk tolerance levels to the business strategy (Curtis & Carrey 2012:Online). It provides guidance on the risk identification process, analysis and risk response areas (IIA 2012), whilst it also addresses the emerging technology risks (Curtis & Carrey 2012:Online).

The COSO framework consists of the following five internal control areas (COSO 2013):

- *Control environment* refers to the control environment determined by the independent board of directors, establishing the standards, structures, reporting lines, ethical values, control processes and assigning organisational responsibilities.
- *Risk assessment* refers to the policies and procedures that identify and analyse the impact and likelihood of risks at all levels, including the risk of fraudulent activities and establishing risk tolerance levels.
- *Control activities* refers to the preventative and/or detective controls implemented in order to reduce the risk levels to an acceptable level in order to achieve the company's strategic objectives.
- *Information and communication* refers to management generating or using quality information for decision-making purposes as well as to internal and external communication techniques used with relevant stakeholders.
- *Monitoring activities* refers to the evaluation of whether the five internal control components have

been implemented effectively. Deficiencies are reported to the board of directors and senior management.

The COSO and ERM frameworks provide the overall internal control framework, whilst the remaining frameworks provide guidance on IT governance related matters (COSO 2013; Curtis & Carey 2012: Online).

4.2.2 COBIT 5 control framework

COBIT 5 is a best practice IT governance control framework which assists management in managing the company's information and technology assets in a holistic manner, including both enterprise wide business and IT functional areas. COBIT defines 37 generic control processes relating to the following two primary process domains (ISACA 2012:Online):

The *Governance* domain refers to the evaluating, directing and monitoring (EDM) of processes. Controls are implemented in order to align IT governance to enterprise governance principles and controls (IT governance network 2011).

The *Management* domain consists of four domains:

i) *Align, Plan and Organise (APO)* focuses on establishing the organisational structures and policies, determine the current and future IT investment strategies, IT internal and external service management policies, implement quality as well as enterprise risk and security management system in order to achieve the company's business objectives (ISACA 2012: Online).
ii) *Build, Acquire and Implement (BAI)* focuses on developing project controls, acquiring IT assets or changes made to the existing information system as well as the implementation of IT asset management and configuration controls (ISACA 2012).
iii) *Deliver, Service and Support (DSS)* focuses on the IT service delivery processes, problem management, implement a business process control framework, design an effective and accurate information system, and ensure the security of IT assets as well as the implementation of a business continuity plan (ISACA 2012).
iv) *Monitor, Evaluate and Assess (MEA)* assesses the effectiveness of the IT system, identify and correct control deficiencies, measure performances against targets, setting goals and comply with the relevant laws and regulations (ISACA 2012).

4.2.3 ITIL control model

ITIL provides guidance to implement an effective and efficient IT service management system. It implements IT governance principles, whilst aligning business and IT objectives. It consists of the following five categories (Cartlidge *et al* 2011; Crown 2011:Online):

i) *Service strategy* provides guidance on transforming service management principles into strategic assets to achieve the company's strategic goals.
ii) *Service design* focuses on the design and implementation of new IT services and changes and improvements to existing services.
iii) *Service transition* provides guidance for building, transitioning and deploying new and changed IT services into operations, whilst controlling the risks of failure and disrupting incidents.
iv) *Service operation* provides guidance on delivering and supporting effective IT services, which addresses user requests, problem management areas and performs routine operational tasks.
v) *Continual service improvement* focuses on maintaining and continuously improving the quality of services delivered through better design, introduction and operation of services and IT processes.

4.2.4 ISO 27001 and ISO 27002

Businesses are increasingly operating in an interconnected environment, implementing emerging technologies such as cloud computing and mobile devices to perform transactions and data transfers. Therefore, data security has become a key risk area for the internal auditor to assess (Ernst & Young 2013:Online). The ISO 27001 forms the foundation in establishing a reliable Information Security Management (ISM) system (Praxiom 2013a:Online) whilst ISO 27002 identifies the corresponding operational controls which must be implemented to mitigate such risks (Kosutic 2010:Online; Praxiom 2013c:Online). By implementing such controls, the confidentiality, integrity and availability of information should be achieved (Praxiom 2013b:Online).

The ISO 27002 control areas are as follows (ISO 27002 2013; PwC 2013:Online):

i) Information security policies provide direction to management to align the information security practices to business and regulation requirements.
ii) Organization of information security establishes a management framework which assigns specific roles and responsibilities to staff, provide security control guidance for project management processes and the use teleworking and mobile devices.
iii) Human resource security provides guidance with regard to change and termination of employee and contractor agreements, security awareness training and disciplinary processes.
iv) Asset management assigns responsibilities to the recording, locations, ownership and acceptable use of assets. Information classification policies based on the importance and sensitivity of information as well as the manner in which media is managed, disposed and physically protected are provided.
v) Access controls provides guidance on controls which grant access to the information assets by controlling access to the user, network, operating system, applications and program source code areas.
vi) *Cryptography* ensures the effective use of cryptography to protect the confidentiality, authenticity and integrity of information, including how to manage generating, protecting, storing,

archiving, distributing and destroying cryptographic keys.

vii) *Physical and environmental security* control policy prevents unauthorized physical access, damage, loss, theft and interruption to a company's information, assets and processing facilities.

viii) *Operations information security* ensures secure information processing facilities through logging and authorizing changes made, separating the development, testing and operational environments, malware protection, sufficient backup procedures, logging of security events, installation of operational systems software as well as evaluating the technical vulnerabilities of the business.

ix) *Communications security* protects information in internal and external networks, establishes policies and service agreements to protect the confidentiality of data transfers in all communication forms.

x) *System acquisition, development and maintenance* implement policies ensuring information security is an integral part of the information system, including application services rendered over public networks and the protection thereof against incomplete transmission and unauthorized changes.

xi) *Development and supporting processes' security* establishing secure development policies (internally and outsourced), system and software change control procedures, development phase testing and performing system acceptance testing whilst ensuring the test data is protected and controlled.

xii) *Supplier relationships* establish information security policies in supplier agreements, detailing the responsibilities of each party and monitoring the compliance thereof.

xiii) *Information security incident management* provides guidance on the effective management and reporting of information security events, the classification, responses and documentation thereof.

xiv) *Business continuity* establishes guidance on the information security requirements, processes, procedures and controls of the business continuity plan.

xv) *Compliance* policies and procedures ensure compliance with the relevant statutory and contractual laws, regulations, security standards, and cryptographic controls, intellectual property rights, protecting records against theft, destruction and loss of data privacy.

4.3 Integrated IT risk assessment questionnaire

The abovementioned control frameworks address different IT control areas. Implementing these best practice control frameworks separately may be tedious, time-consuming, paper intensive and require significant resources, resulting in a cost intensive exercise (Rudman 2008:12-14).

However, by developing a single integrated questionnaire, it can be based on updated, renowned and internationally recognised frameworks in assisting the internal auditor to assess high level key IT risks. It can also be customised based on the company's unique business requirements, whilst costs are optimised by using a standardised, rather than a specifically developed approach. The questionnaire also ensures that IT governance related matters are complied with whilst ensuring an effective internal IT risk assessment is performed. Due to the increased implementation of emerging technologies such as big data and the use of external parties such as cloud providers, it is important to understand the risks such complex IT environments entail. The authenticity and integrity of data obtained from various sources inside and outside the IT environment must, therefore, be adequately protected. It also ensures compliance with the latest laws and regulations applicable to the changing IT environment, including privacy and financial reporting standards (Hardy 2006:55-61; ISACA 2012:Online & NCC 2005:Online). By combining the high level key IT control areas of the abovementioned control frameworks, the integrated IT risk assessment questionnaire was developed.

5 INTEGRATED IT RISK ASSESSMENT QUESTIONNAIRE

The following high-level IT related questions were identified, which could assist the internal auditor to pose the correct questions to IT and risk management, thereby ensuring that key high level IT risks are appropriately assessed in a business' IT environment in a methodical and structured manner. The questionnaire is divided into key high level risk areas, which can either be performed once every few years (Part A: non-annual) or annually (Part B), if the risks or the specific industry's risk environment changes more regularly.

Table 1: Integrated IT risk assessment questionnaire

A Non-annual questions

1. IT governance strategy: What are the company's policies and procedures encompassing: • overall corporate governance matters (e.g.: the integrity, philosophy and ethical values)? • how IT governance matters are incorporated into the corporate governance structures? • the board of directors' roles, responsibilities and understanding of IT-related matters? • delegating responsibilities relating to risk management and IT governance matters? • the level of experience and independence of the IT steering and risk committees? • the general IT control environment relating to the systems, infrastructure and process areas? • the role and responsibilities of the Chief Information Officer (CIO)? • the CIO's reporting responsibilities to the board, steering committee and audit committee? • the frequency through which emerging technology risks are assessed? • the standard of the reviews performed on IT control processes?

2. IT risk management: What are the company's policies and procedures encompassing:

- the risk philosophy, appetite and tolerance levels? Is it appropriate given the company's risk profile?
- the alignment between the IT risk strategy and the strategic business objectives?
- the establishment of the Enterprise Risk Management (ERM) system?
- the timely identification of new key IT risks and the update of the risk register?
- the documentation and communication thereof to employees and other stakeholders?
- the consideration of the external and internal IT factors in the risk assessment process?
- the identification of key risk related IT processes and IT assets?
- the prioritization and ranking of key IT risks based on its potential impact, likelihood and level of vulnerability?
- the documentation and assignment of risk responses to a responsible person?

3. Project management: What are the company's policies and procedures encompassing:

- the general control environment relating to key IT processes, access, application and configuration settings which are either acquired, developed or updated?
- the project approval process?
- the appropriate level of involvement of the IT users, CIO, IT steering committee, internal and external auditors and the board of directors at each development stage?
- the adequate updating and documentation of system analysis, programme specifications, all changes and new developments made?
- the implementation of a formal project plan, ensuring quality reviews, specific standards, coding methodologies and correction processes at each development stage?
- the appropriate composition of the project team and granting access rights?
- testing the system's integrity including data clean up, transfer of data and resolving discrepancies during the conversion phase?
- the adequate conversion, backup and post-conversion processes? How are exceptions identified and resolved?

4. Compliance management*:* Which laws and regulations, specifically relating to IT-matters need to be complied with including:

- corporate and IT governance matters, sector specific regulations and security policies;
- legal contracts such as intellectual property arrangements, trademarks, licences, copyrights and service level agreements;
- electronic communication, cloud based information systems, e-commerce regulations, information security and privacy regulations; and
- document and record retention, development and technical compliance standards and cryptographic regulations?

B. Annual questions

1. ***IT organisational management:*** What are the company's policies and procedures encompassing:

- assigning appropriate levels of authority, access rights and segregation of duties to employees and other stakeholders?
- the adequate segregation of duties between the IT and user departments as well as within the IT department function?
- the appropriate levels of training received by IT users?
- communicating the appropriate use of IT hardware and software assets and its related risks to employees and other stakeholders?
- granting new users access to the IT system and removing access rights of employees who have retired/contracts terminated in a timely manner?
- no undue reliance placed on key IT personnel and appropriate staff rotation schedules?

2. IT Resource and investment management: What are the company's policies and procedures encompassing:

- the procurement standards and supplier and service delivery agreements that are in place? Are these policies aligned to the disaster recovery plan?
- the operations and the control environment of outsourced IT services?
- essential terms and conditions included in the outsourced contracts, such as non-performance and liability clauses, minimum security control requirements and obtaining the independent assurance qualification review of such service providers?

3. IT service management: What are the company's policies and procedures encompassing:

- supporting the internal IT services, providing the disaster recovery plan and aligning it to the overall business strategy?
- managing the centralised service desk activities, the resolution and documentation of all problems and security incidents? Are the root causes identified, analysed, categorized and prioritized in order to be resolved?
- ensuring the personnel, who manage and maintain the technical infrastructure and software system applications, have the appropriate level of expertise?
- the identification of suitable external service providers (e.g.: cloud service providers)? Have the cloud policies been integrated with the legal, procurement and IT policies?

4. Access management: What are the company's policies and procedures encompassing:

- the physical access controls, protecting IT assets against physical and environmental dangers?
- ensuring a secure physical location of important IT assets such as data centres, servers, programmes and the protection of the power supply and cabling?
- the use of logical access controls to ensure that appropriate level of access rights are granted? Are these controls implemented in at least the following areas namely: systems, programmes, critical system files, Structured Query Language (SQL) server data directories and at wide and remote access levels?
- the password policies being implemented?
- the implementation of preventative, detective and corrective access controls such as anti-virus software, firewalls and logs, library and file protection controls to protect the information systems from malware attacks?
- the identification of sensitive data, the location and transfer of such data?
- the data communication and exchange controls (both physical and electronic) that are in place, ensuring the integrity of transferred data?

• the data transfers to and from external service providers? • the type of data transfer devices which are allowed, including remote, mobile and bring-your-own-devices? • lost or stolen devices? • the appropriate type of communication lines used? • the encryption and cryptographic controls ensuring data security? • the use of e-commerce websites? If used, what access controls are in place with regard to the order and sales transactions, sensitive customer data and data transfers to the primary information system? • the effectiveness of the website's anti–intrusion controls? • the logging and reporting of changes to access rights and sensitive transactions, overridden controls , IT components' access points and unauthorised entrances? • the exception report review process, the communication policies of critical access exceptions and the processes to resolve such matters?
5. Business Continuity management: What are the company's policies and procedures encompassing: • how critical systems are defined, identified and included in the disaster recovery plan? • the IT disaster recovery plan and are the financial strategic goals also incorporated? • the company's backup policies and procedures? • the extent of the supplier and service level agreements, especially relating to e-commerce and cloud computing service providers? • the authentication protocols in place for cloud users?
6. Configuration management: What are the company's policies and procedures encompassing: • the business risk impact studies conducted by making use of cloud services and other emerging technologies (e.g.: mobile and bring-your-own-devices)? • how these emerging technologies increase the level of open and remote access as well as the risk of unauthorized access? • the configuration controls implemented over mobile devices? • ensuring all critical access points relating of IT assets, networks and systems are identified and risk managed? • the identification of any unknown open access points relating to IT assets and networks? • the authentication settings and operating control systems? • the determination of the correct configuration settings of user endpoints and shared network connections?
7. Application management: What are the company's policies and procedures encompassing: • operational, technical and organisational IT processes and controls to manage the flow of information between functional areas? • how transactions are initiated, recorded, processed and reported? • the input, processing, output, master-file amendments and databases controls which ensure the integrity, accuracy, confidentiality, availability, authenticity and non-repudiation criteria of information? • the appropriate code used in mobile applications?

The abovementioned questionnaire should provide a sound foundation and direction to the internal auditor to ensure that the appropriate questions are asked, as well as identifying the relevant key IT risk areas, which have been appropriately addressed, by the risk and IT management teams.

7 CONCLUSION

Due to the complex nature of the IT environment within which companies function today, the assessment of IT risk-related matters has become a significant area of concern for the internal auditor. Most of the well-known frameworks used by the internal auditor have also been updated recently and focus areas changed to include the risks of utilising emerging technologies in the IT environment. However, the internal auditor needs assistance to keep abreast with these changes to the relevant frameworks and could lack sufficient IT knowledge in how advanced its IT systems and emerging technologies impact the risk assessment process. This article analysed these updated best practice IT and risk control frameworks in order to develop an IT risk assessment questionnaire, which could assist the internal auditors to conduct an effective internal risk assessment of the high-level key IT risks. By utilising the questionnaire, only one condensed and combined guidance tool can be used, instead of consulting the individual frameworks, which contain a vast amount of detail, some irrelevant information for the internal auditor's purposes while certain processes are discussed repetitively. This integrated approach could reduce the amount of time and cost spent conducting risk assessment procedures, whilst ensuring the internal auditor asks the correct questions, which includes; the evaluation of the risks emerging technologies pose to a modern day IT environment.

REFERENCES

Ali, S.M., Soomro, T.R. & Brohi, M.N. 2013. Mapping information technology infrastructure library with other information technology standards and best practices. *Journal of Computer Science*, 9(9):1190-1196.

Basti, P. 2015. *KPMG Internal audit: top 10 key IT risks in 2015.* [Online]. https://www.kpmg.com/US/en/IssuesAndInsights/ArticlesPublications/Documents/top-10-considerations-internal-audit-2015.pdf (Accessed: 30 May 2016).

Broadleaf. 2014. *Relationship between internal audit and risk management.* [Online]. http://broadleaf.com.au/resource-material/relationship-between-internal-audit-and-risk-management. (Accessed: 30 May 2016).

Cartlidge, A., Rudd, C., Smith, M., Wigzel, P., Rance, S., Shaw, S. & Wright, T. 2011. *An introductory overview of ITIL 2011.* [Online]. http://www.doc-developpement-durable.org/file/Projets-informatiques/cours-&-manuels-informatiques/ITIL/An_Introductory_Overview_of_ITIL_V3.pdf (Accessed: 10 June 2016).

Committee of Sponsoring Organizations of the Treadway commission (COSO). 2013. *Internal control – integrated framework.* [Online]. http://207.248.177.30/mir/uploadtests/31233.177.59.1. COSO%20III_2013.pdf (Accessed: 14 September 2015).

Crown. 2011. *ITIL 2011 Summary of updates*. [Online]. http://media.cms.bmc.com/documents/ITIL_2011_Summary_of_Updates.pdf (Accessed: 10 June 2016).

Curtis, P. & Carey, M. 2012. *Thought leadership in ERM. Risk assessment in Practice.* [Online]. http://www.coso.org/documents/COSOAnncsOnlineSurvy2GainInpt4Updt2IntrnlCntrlIntgratdFrmwrk%20-%20for%20merge_files/COSOERM%20Risk%20Assessment%20inPractice%20Thought%20Paper%20OCtober%202012.pdf (Accessed: 10 June 2016).

Elhasnaoui, S., Medromi, H., Faris, S., Iguer, H. & Sayouti, A. 2014. Designing a multi-agent system architecture for IT governance platform. *International journal of advanced computer science and applications*, 5(5):157-161.

Ernst & Young. 2013. *Ten key IT considerations for internal audit.* [Online]. http://www.ey.com/Publication/vwLUAssets/Ten_key_IT_considerations_for_internal_audit/$FILE/Ten_key_IT_considerations_for_internal_audit.pdf. (Accessed: 30 May 2016).

Galligan, M.E. & Rau, K. 2015. *COSO in the cyber age.* [Online]. http://www.coso.org/documents/COSO%20in%20the%20Cyber%20Age_FULL_r11.pdf (Accessed: 10 June 2016).

Gheorghe, M. 2010. Audit methodology for IT governance. *Informatica Economica*, 14(1):32-42.

Hardy, G. 2006. Using IT governance and COBIT to deliver value with IT and respond to legal, regulatory and compliance challenges. *Information security technical report*, 11:55-61.

Huawei Technologies. 2013. *NAC Technology White paper*. [Online]. http://www.google.co.za/url?sa=t&rct=j&q=&esrc=s&frm=1&source=web&cd=1&ved=0CCoQFjAA&url=http%3A%2F%2Fwww.huawei.com%2Filink%2Fenenterprise%2Fdownload%2FHW_201021&ei=DU5uUurmK4yVhQfr4YHoCA&usg=AFQjCNFYbFM4354_kiBOAvYn3mhHnFMfDw&sig2=hut8UcVoVc4tSEMHM87nWg&bvm=bv.55123115,d.Yms (Accessed: 10 June 2016).

Institute of Directors Southern Africa (IODSA). 2009. *King Report on corporate governance for South Africa. SAICA Legislation handbook 2010/2011. Volume 3.* Durban: LexisNexis.

Institute of Internal Auditors (IIA). 2012. *Auditing IT governance*. [Online]. http://iia.nl/SiteFiles/IIA_leden/Praktijkgidsen/GTAG%2017%20Auditing%20IT%20Governance[1].pdf (Accessed: 10 June 2016).

Institute of Internal Auditors (IIA). 2009. *The role of internal auditing in enterprise-wide risk management.* [Online]. https://na.theiia.org/standards-guidance/Public%20Documents/PP%20The%20Role%20of% 20Internal%20Auditing%20in%20Enterprise%20Risk%20Management.pdf. (Accessed: 30 May 2016).

ISACA & Protiviti. 2014. *A global look at IT audit Best practices.* [Online]. http://www.protiviti.com/en-US/Documents/Surveys/4th-Annual-IT-Audit-Benchmarking-Survey-ISACA-Protiviti.pdf (Accessed: 10 June 2016).

ISACA. 2012. *COBIT 5. Enabling processes*. [Online]. http://www.isaca.org/cobit/pages/cobit-5-enabling-processes-product-page.aspx (Accessed: 10 June 2016).

ISACA. 2014. *Relating the COSO internal control integrated framework and COBIT.* [Online]. http://www.isaca.org/knowledge-center/research/researchdeliverables/pages/relating-the-coso-internal-control-integrated-framework-and-cobit.aspx (Accessed: 10 June 2016).

ISO/ IEC 27002. 2013. *International standard ISO 27002.* [Online]. https://trofisecurity.com/assets/img/ISO-IEC_27002-.pdf (Accessed: 10 June 2016).

IT Governance Institute (ITGI). 2008. *COBIT Mapping*. *Mapping of ITIL v3 with COBIT 4.1.* [Online]. http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/COBIT-Mapping-

Mapping-of-ITIL-V3-With-COBIT-4-11.aspx (Accessed: 10 June 2016).

IT governance network. 2011. *Summary of differences between COBIT 4.1 and COBIT 5.* [Online]. http://www.qualified-audit-partners.be/user_files/COBIT5forAuditors/Summary_of_differences_between_CobiT_4_1_and_CobiT_5-2012-IT_Governance_Network.pdf (Accessed: 10 June 2016).

Kosutic, D. 2010. *ISO 27001 vs ISO 27002*. [Online]. https://www.infosecisland.com/blogview/8055-ISO-27001-vs-ISO-27002.html (Accessed: 10 June 2016).

Liell-Cock, S., Graham, J. & Hill, P. 2009. *IT governance aligned to King III*. [Online]. http://lgict.org.za/document/it-governance-aligned-king-iii (Accessed: 10 June 2016).

National computing centre (NCC). 2005. *IT governance. Developing a successful governance strategy*. [Online]. https://www.isaca.org/Certification/CGEIT-Certified-in-the-Governance-of-Enterprise-IT/Prepare-for-the-Exam/Study-Materials/Documents/Developing-a-Successful-Governance-Strategy.pdf (Accessed: 10 June 2016).

Praxiom. 2013a. *ISO IEC 27001 2013 Annex A*. [Online]. http://www.praxiom.com/iso-27001-annex-a.htm (Accessed: 10 June 2016).

Praxiom. 2013b. *ISO IEC 27002 2013*. [Online]. http://www.praxiom.com/iso-27002-overview.htm (Accessed: 10 June 2016).

Praxiom. 2013c. *ISO IEC 27002 Old versus new.* [Online]. http://www.praxiom.com/iso-27002-old-new.htm (Accessed: 10 June 2016).

Protiviti. 2013. *The updated COSO internal control framework.* [Online]. http://www.protiviti.com/en-US/Documents/Resource-Guides/Updated-COSO-Internal-Control-Framework-FAQs-Third-Edition-Protiviti.pdf (Accessed: 10 June 2016).

Protiviti. 2014. *Assessing the top priorities for internal audit functions.* [Online]. https://www.protiviti.com/en-US/Documents/Surveys/2014-Internal-Audit-Capabilities-and-Needs-Survey-Protiviti.pdf. (Accessed: 30 May 2016).

PwC. 2013. *New releases of ISO 27001:2013 and ISO 27002*. [Online]. https://www.pwc.com.cy/en/publications/assets/iso27001-27002-2013.pdf (Accessed: 10 June 2016).

Rudman, R.J. 2008. IT governance: a new era. *Accountancy SA*, March:12-14.

Santarcangelo, M. 2010. *Configuration auditing – the next critical step in compliance.* [Online]. file:///D:/Downloads/http---www.networkworldme.com-ms-fvc2011-wp-content-uploads-2011-06-nCircle-WP-ConfigurationAuditingNextStep-1064-03.pdf (Accessed: 10 June 2016).

Steenkamp, G. 2011. The applicability of using COBIT as a framework to achieve compliance with the King III Report's requirements for good IT governance. *Southern African Journal of Accountability and Auditing Research*, 11:1-8.

Svata, V. 2013. System view of Business continuity management. *Journal of system integration*, 2:19-35.

The Southern African Journal of Accountability and Auditing Research

Evolving Research

Risks associated with corporate social media communication – Time for internal auditing to step-up

SC Green

Department of Auditing
University of Pretoria

ABSTRACT

Various case studies highlight the negative effect corporate social media communication risks have on organisations. In this study, the risk associated with corporate social media communication in organisations is investigated. The extent of internal auditing's involvement to assist management in evaluating and mitigating the risks that such communication poses is also explored. The study revealed that organisations' brand and reputation is the most important risk. A significant number (33%) of respondents indicated that risk of social media communication were not included in their organization's internal audit universe. The majority indicated that internal auditing did not evaluate or was not trained to evaluate the effectiveness of corporate social media communication controls. The results of this study revealed that there are opportunities for internal auditing to focus its efforts on becoming involved in evaluating risks relating to corporate social media communication.

Key words

Corporate social media communication; risks; internal auditing; mitigation

Acronyms

IIA SA	Institute of Internal Auditors South Africa (IIA SA)
IPPF	International Standards for the Professional Practice of Internal Auditing

1 INTRODUCTION

Corporate social media communication, including Twitter, Facebook, Instagram, WhatsApp, SMS, emails, Mxit, Skype, BBM and Snapchat, has become a growing trend across the globe. This trend is growing exponentially, according to Baker, Buoni, Fee & Vitale (2011), therefore, there are also an increasing number of risks associated with these trends. This necessitates that organisations ensure that they are aware of and fully understand the risks they face in a corporate social media communication environment.

Based on a 10% share price drop at Domino's Pizza as a result of a reputational risk consequence, Tony Sousa, Chief Executive Officer of Acceleration Media, stated that one does not have control over people discussing ones organisation, brand or products in an online environment (Media News 2012:Online). Organisations' service, financial performance, ethics and products are under constant scrutiny and people make use of various social media communication tools to voice their opinions, whether merited and corroborated or not (Our Social Times 2013:Online). These social media communication tools reach a widespread base of connected customers and can easily result in a minor customer complaint today being a newspaper headline tomorrow.

Internal auditing, as defined by the Institute of Internal Auditors South Africa (IIA SA 2012:Online), is mandated to assist management in identifying and mitigating risks as the value-adding factor of the internal audit activity (IIA 2012:Online). This implies that internal auditing has two important tasks: firstly, to understand the corporate social media communication environment and secondly, to assist management in identifying and mitigating the relevant risks being faced by the organisation in this regard.
This article addresses the various risks associated with corporate social media communication and the negative impact these risks can have on an organisation. This is done through a review of relevant case studies. The importance internal auditing plays in assisting management to mitigate these risks is then further investigated, followed by a discussion of the results of the empirical research. Finally, in the conclusion, possible areas to step-up internal auditing are briefly highlighted to assist management with the mitigation of risks associated with corporate social media communication.

2 RESEARCH PROBLEM, OBJECTIVES AND LIMITATIONS

2.1 Research problem

According to Recalde (2010:2), unmanaged risks associated with the use of corporate social media communication by employees, colleagues or third parties could result in management facing liability claims such as defamation, online criticism, infringement of

privacy or publicity rights, interference with advantageous economic relations, misrepresentation and infringement of intellectual property rights, and false advertisement or unfair competition, to name but a few.

In a 2012 survey of 192 United States executives, corporate social media communication is identified as the fourth largest risk (Deloitte & Forbes Insights 2013:Online). The importance of corporate social media communication risks cannot be over-emphasised.

In addition, research conducted by Mushwana and Bezuidenhout (2014) reveals that only 38% of the respondents in their study had a social media policy in place. The absence of a formal policy is not necessarily an indication that organisations did not employ informal rules and protocols pertaining to the use of social media in the workplace. It is, however, evident that most organisations do not realise the significant impact such a risk might have. In most instances, a crises is the trigger for putting in place policies on social media, which is often too late because substantial reputational and subsequent financial damage may have already occurred. The potential damage to reputation may be done when employees use social media to express their dissatisfaction with an organisation's views and policies or with specific supervisors or executives. Organisations usually respond to these cases with the strongest possible sanctions.

The literature revealed that the risks associated with the use of social media are not currently prioritised in organisations' audit risk universe. According to Mushwana & Bezuidenhout (2014), only 24% of the companies questioned in its study had dedicated programmes in place to monitor and mitigate these type of risks.

Based on the review of a number of relevant case studies (Gordon 2007:Online; Aula, Laaksonen & Neiglick 2010:Online; Recalde (2010:2); Anderson *et al* 2011:Online; Merrill *et al* 2011; Osborne 2011: Online; Fleming & Miles (2012:7); Media News 2012: Online; Cavico *et al* 2013; Magcaba 2013:Online; McCorkindale & DiStaso (2013:499); Our Social Times 2013:Online; Mushwana & Bezuidenhout 2014; Mybroadband 2014:Online) regarding the negative effects and risks of corporate social media communication, as well as previous research conducted on the absence of formal policies that address these risks in organisations, it appears that there is room for improvement in the services provided by the internal audit activity. What comes to mind is the value internal auditing can add to its organisations by enhancing its role in assisting management to identify these risks and to mitigate them (Singleton 2012:Online; Bogoslaw 2014:Online; Brinkley 2014; Culp 2014:Online; Roath & Holcomb 2014:Online).

The internal audit activity provides assurance to management and the audit committee that risks in the organisation are understood and properly managed. It involves the identification of risks in the organisation and the identification and implementation of risk mitigation plans (IIA 2012:Online). As mentioned above, the risks associated with poor corporate social media communication can have a significant negative impact on an organisation.

Against the aforementioned background, a study was conducted to investigate the role of internal auditing in providing assistance to management in mitigating the risks associated with corporate social media communication.

2.2 Research objectives

In an attempt to address the research problem and the purpose of the study, the objectives of the research were:

1 to determine, through a review of case studies, the various risks, effects and challenges that corporate social media communication poses for organisations; and
2 to explore the extent of the involvement (i.e. the role) of internal auditing in assisting organisations' management to evaluate and mitigate the risks that corporate social media communication poses.

This study aims to raise awareness among organisations and chief audit executives on how internal auditing can assist them in mitigating these risks. By helping management to identify and mitigate these risks, internal auditing will, in the long term, add value to any organisation. This value-adding factor of internal auditing is included in its definition as prescribed by the IIA SA. Internal audit activities in organisations will also be able to assess whether internal auditors are involved to a sufficient extent and adequately trained to evaluate the effectiveness of risks associated with corporate social media communication in organisations.

2.3 Research limitations

The research did not focus on any positive or advantageous use of corporate social media communication.

Case studies were selected from the literature review according to their relevance.

3 RESEARCH DESIGN AND METHODOLOGY

The methodology adopted for this article was based on a quantitative approach. Creswell (2003:18) describes the quantitative approach as a process in which the investigator uses post-positivist claims to develop knowledge. Strategies such as experiments and surveys are employed to collect statistical data through predetermined instruments. According to Castellan (2010:Online), quantitative researchers gather data through questionnaires, tests and surveys. The data is analysed by means of a deductive process and statistical procedures.

In further pursuit of reaching the second research objective stated in section 2.2., a high-level literature review was also conducted to obtain a better understanding of the involvement of internal auditing in assisting management in mitigating the risks associated with corporate social media communication.

3.1 Questionnaire

The research was extended to include an empirical study which was conducted by means of a structured self-administered questionnaire. This questionnaire explores the extent of the involvement (i.e. the role) of internal auditing in assisting organisations' management in evaluating and mitigating the risks that corporate social media communication poses. The questionnaire was distributed via the South African chapter of the IIA. The IIA SA newsletter was used to circulate the internet link to the questionnaire requesting potential respondents to complete online. A covering letter containing the objective of the research was also distributed with the questionnaire. The questionnaire covered the following three focal areas and is attached as Annexure A:

- the development of corporate social media communication in organisations;
- the responsibility and monitoring of risks of corporate social media communication; and
- the involvement of internal auditing in assisting management in mitigating these risks.

3.2 Population and sample

The target population is an aggregate of all the elements pertinent to a study, an idealised group representing the totality of target elements that interest a researcher (Smith 1988:77). Applied to the present study, it refers to the database of members of the South African chapter of the IIA SA.

3.3 Reliability and validity

The questionnaire was peer-reviewed by the author's supervisors and various colleagues in the field of internal auditing with reference to its objective, logic, meaningfulness and ambiguity of the questions. Twenty closed-ended questions were posed.

3.4 Data analysis

In this study, an analysis of frequency tables was used to discuss one independent variable at a time, and cross-tabulations were used to describe the relationship between two independent variables (Babbie 2009:436-440).

Thirty respondents submitted completed questionnaires via electronic mail.

The data was scrutinised for accuracy and completeness before the results were captured on Moonstats, which is a statistical analysis software program supplied by Wellman and Kruger (2001). The program allows the researcher to perform an analysis of frequency tables to discuss one independent variable at a time and to use cross-tabulations to describe the relationship between two independent variables.

4 LITERATURE REVIEW

Brogan (2010) and Zarella (2010) defined social media as "media designed to be disseminated through social interaction between individuals and entities such as organisations." The techniques used to publicise this media must be easily accessible and should be able to reach a substantial number of people. It includes interactive communication, socialising and sharing emails, documents, pictures, videos, audio files, and each can be done in a number of different ways.

According to Hudson and Roberts (2012:769), the terms "social media" and "social networking" are used synonymously, but the former refers to the means by which communications are transmitted, while the latter refers to the functional tools used for information-sharing. Facebook, LinkedIn, MySpace and Twitter have been identified by Baker *et al* (2011) as the four most popular and commonly used social networking sites. Furthermore, Ployhart (2014) highlighted the use of social media as a growing trend whose power cannot be ignored. To summarise, social networking is the transmitting of messages via a variety of electronic media devices for the purpose of sharing information with society on all levels.

The use of social networking in a corporate environment refers to the activities of both employer and employees within the business. A corporation has, like a private person, a legal entity and can be sued, commit crimes and be punished (Business Dictionary, n.d:Online).This implies that the business can be held responsible for social networking activities linked to the corporation.

4.1 Risks of corporate social media communication

From the literature, and consistent with the first research objective in section 2.2., various risks were identified as inherent in corporate social media communication. A high-level analysis of various case studies (randomly selected) enabled the identification of the following risks (which are discussed below) as well as the negative impact they have on organisations. i.e. reputational, compliance, data information leakage, third party & productivity risk.

Reputational Risk

This risk involves an organisation suffering loss or foregoing possible business opportunities as a result of the relevant shareholders or the public losing faith in the organisation's character, integrity or quality of operations. This loss of faith can be based on an opinion or perception and does not necessarily mean that it is correct or that the organisation is guilty (McCorkindale & DiStaso 2013).

Warren Buffet, a successful and well-known American business magnate, investor and philanthropist, made the following impactful statement: "It takes 20 years to build a reputation and five minutes to ruin it, if you think about that, you'll do things differently" (Berman 2014:Online).

There are several real-life examples in organisations that underline the fact that the reputation of an organisation can be damaged in the blink of an eye as negative posts spread virally throughout the world. Below are examples which highlight the negative effect and consequences of reputational risk:

- Employees at a Domino's Pizza store posted a video on YouTube that showed how they inappropriately and unhealthily prepared pizzas for their clients. This resulted in the organisation's share price dropping by 10% soon after the post (Media News 2012:Online).
- Aula *et al* (2010:Online) discussed a case in which Nestlé's Facebook page was hi-jacked by Greenpeace. They changed the Nestlé Kit Kat Logo to Nestlé "Killer" as a campaign against Nestlé's use of palm oil. Nestlé's subsequent reaction led to more controversy and caused additional brand damage to the organisation.
- Mushwana and Bezuidenhout (2014) refer to the First National Bank case in which the organisation unwittingly caused serious reputational damage and the employee involved exposed himself to further disciplinary action. Their organisation's Twitter account used in an advertising campaign made insensitive remarks on Twitter about their "Steve" character, requiring the company to do serious damage control (Mybroadband 2014:Online). Mushwana and Bezuidenhout (2014) also mentioned a case in which two South African employees of the For Him Magazine posted offensive comments about "corrective rape" on Facebook, leading to their dismissal (Magcaba 2013:Online).
- Our Social Times (2013:Online) reported on the case of Applebee's restaurant, where an employee took a cell phone picture of a negative remark that a customer wrote on a receipt. The picture was posted on the social media webpage Reddit. The employee was subsequently fired for violating customer privacy. What made matters worse was when, in their defence of the aforementioned matter, the restaurant posted another receipt on which a customer wrote, complimenting their service. This defensive approach resulted in over 10 000 mostly negative comments posted by social media communication users.
- In another instance, thirteen Virgin Atlantic employees attempted to discredit the organisation by posting a comment on Facebook stating that the planes were full of cockroaches. They were subsequently fired (Fleming & Miles 2012:7; Cavico *et al* 2013).

It is clear from the above-mentioned case studies that reputational risk poses a great threat to corporate social media communication. To substantiate this, McCorkindale and DiStaso (2013:499) hold that the biggest risks for an organisation, when it comes to the power of social media, lies in that organisation's reputation in terms of its services or products, and in their perceived public image.

Compliance Risk

The risk is created by the violation of the legislative and regulatory framework within which a company operates. This includes laws, regulations, standards and prescribed practices. The result of non-compliance can result in increased reputational risk (Enlightenme n.d.:Online).

Kelsey and Mattossian (2004:Online) define compliance risk as:

> [*t*]he adverse consequences that can arise from systematic unforeseen, or isolated violations of applicable laws and regulations, internal standards and policies and expectations of key stakeholders including customers, employees and the community, which can result in financial losses, reputation damage, regulatory sanctions and in severe cases loss of franchise or rejected mergers and acquisitions.

An organisation should have in place strict internal policies and frameworks of corporate social media communication to ensure that employees are aware of and legally bound to these policies. The lack of such policies and frameworks might cost the organisation in civil claims and reputational damage (Recalde 2010:2). The legislative and regulatory framework forms an integral part of all organisations and companies and forms the backbone of its activities. It is, therefore, essential that policies for the use of social media be drafted, implemented and adhered to.

Data or information leakage risk

This risk realises as a result of unauthorised external sharing of information or data belonging to the organisation (Gordon 2007:Online). The leakage can take the form of manual or electronic transmission and might not necessarily have been done deliberately or with any malicious intent. However, the fact that it was not done deliberately does not condone the data or information leakage. Data or information can be leaked from internal sources in the organisation or external sources, such as hackers (Gordon 2007:Online).

Zurich (2008:Online) states in an article that costs associated with information security breaches increase annually. Expenses arise from customer notification, audit costs, call centre expenses, and credit monitoring and legal fees. The indirect costs arise from a loss of reputation and productivity as well as litigation fees. It is, therefore, imperative for companies to have risk management strategies in place.

According to Gordon (2007:Online), most companies have trade secrets and confidential information. Should this information be public knowledge, the organisation can suffer severe losses. The availability of cell phones with cameras and access to databases and emails makes the circulation of confidential information relatively simple. As a result, an organisation needs to put in place rigid measures to prevent information leaking from the inner workings of the organisation through corporate social media communication. Osborne (2011:Online) discusses a rather ironic case in which Apple's policies on social networking and blogging. The guidelines outlined how its employees should conduct themselves and not leak data. However, data was leaked by an employee who was subsequently dismissed. Osborne (2011: Online) also highlighted how this incident illustrated that policy alone will not deter employees from leaking information.

The use of photos and intellectual property of individuals and organisations on an organisation's social media page might also cost them dearly if the necessary permission is not obtained (Our Social Times 2013:Online). Our Social Times (2013:Online), reported that Donna Karan New York, a New York-based fashion house used a photographer's photographs in a window display without his permission. The photographer noticed that it was his photos and asked the organisation to make a substantial donation to a welfare organisation. The organisation settled for a lower amount but still had to pay a substantial amount for the violation. Such unlawful uses of trademark or copyright on social media can unwittingly lead to civil claims and reputational damage to the organisation (Our Social Times 2013:Online).

For any business to be competitive, most if not all information, including financial statements, is stored electronically. Access to this information, be it authorised or unauthorised, can leave the company open to various risks, the most prevalent of which are fraud, reputational and legal (copyright and trademark) risks (Walter 2006:Online; Zurich 2008: Online).

Third-Party Risks

Jurgens (2013:Online) asserts that third-party risks arise because of the negative relationships to which the organisation is exposed along with their external stakeholders, such as service providers, suppliers and other delivery partners. This risk is increased when affiliated third party marketers do not comply with the applicable laws that govern advertising and marketing activities.

Deloitte (2014:Online) argues that third-party risk has become increasingly important and should be managed on several levels. Third-party risks are ever-increasing as companies outsource many of their functions to third parties, including overseas companies primarily for strategic and financial reasons. However, this practice brings with it risks regarding regulatory issues, reputation and data security.

In the banking sector, a third-party relationship would include out-sourced products and services, the use of independent consultants, networking arrangements, merchant payment processing services, etc. The bank has an on-going relationship with or may have a responsibility towards the associated records (KPMG 2014:Online).

There are various internal and external challenges facing organisations when developing risk strategies and metrics to address the wide variety of third-party relationship risks as identified by Anderson *et al* (2011:Online). Internal challenges include ownership of risk responsibilities, a reactive approach to risk management and traditional metrics that do not include risk. The external challenges include complex, global supply chains, new disclosure expectations that increase exposure to reputational risk and complex invoicing.

An organisation should keep abreast of the power of social media in its governance structures. Aula *et al* (2010:Online) illustrated this by discussing a case in which the Financial Times refused to publish an advertisement about the "gas flaring practices" of Shell's Organisations. Amnesty International used the advertisement to their advantage by posting it on Facebook and Twitter and obtained 62 000 hits in a month. The Financial Times' refusal to post the advertisement cost them dearly in exposure and sales.

A study conducted by Chain Link Research, quoted by Anderson *et al* (2011:Online) revealed that nearly 50% of the organisations indicated that risk assessment played the most critical role in their service provider selection. However, more than 70% of the surveyed organisations reported having no resilience and risk-mitigation standards to which they hold their service providers. The study also noted that the quality of the risk assessments performed depended on the organisations' capacity and competence to identify these risks.

When an organisation or company outsources functions and services, it is bound to lose some control of not only that specific function or service but also of its reputation because the contracted service provider will be associated with the holding company and will also determine their ability to deliver. Contracts should, therefore, be thorough and specific.

Productivity Risk

This risk that is often overlooked refers to the potential decrease in productivity of employees (Cavico *et al* 2013).

Ferreira and Du Plessis (2009) list addictive behaviour that can be developed leading to lower productivity as one of the several risks associated with the use of social media in the workplace. Aguenza and Puad Mat Som (2012:Online), in their research, came to the conclusion that the use of social media in the workplace results in several risks in employee productivity, namely: possible data leakage and security breaches. However, there are more positive outcomes as social media can be used as an extremely effective internal and external communications medium. The use of social media also promotes openness, diversity and respect. The key to social media in the workplace lies in the strict implementation of policies and strategies to increase the benefits of social media.

For organisations, the practical implication of productivity risk is the possibility of a drop in employees' productivity due to the uncontrolled use of social media devices. Cavico *et al* (2013) make reference to research conducted in 2009, wherein 77% of the employees accessed their Facebook accounts for personal reasons during office hours. They also found that the average employee accessed the internet for personal reasons for between one and two hours a day. Wilson (2009:Online) reports that the amount of time their employees spend on social websites during working hours is a concern to management and executives. According to Greenwald (2009:Online), 55% of the employees visit a social networking site at least once per week. This phenomenon is difficult to control because employees do not necessarily use the organisation's equipment to access social media,

but their private devices. It may be viable to allow employees to access their social media networks during their predetermined breaks. A strict but fair policy should be agreed upon by both management and employees (Merrill *et al* 2011).

From the literature discussed above as well as the case studies analysed, it was possible to draft the following table (Table 1), summarising the risks that can most commonly be found in the corporate social media communication environment:

Table 1: Summary of risks most commonly found relating to corporate social media communication

Case study	Risk identified
Domino's Pizza	Reputational risk
BP / Greenpeace / Nestlé	Reputational risk
First National Bank	Reputational and legal claim
Applebee's restaurant	Reputational risk
Virgin Atlantic	Reputational risk
For Him Magazine (South Africa)	Reputational risk
Apple	Data or information leakage risk
DKNY (Donna Karan New York)	Data or information leakage risk and reputational risk
Shell	Third-party risk

4.2 Key challenges facing organisations in corporate social media communication and possible solutions

Organisations face various corporate social media communication challenges. The key challenges facing organisations is the lack and implementation of policies and the manner and timing of the responses when a crises arises.

The results of the survey conducted by Deloitte LLP revealed that organisations do not take social media networking seriously with regard to policy development, implementation and adherence.

It was further highlighted by Mushwana and Bezuidenhout (2014) that although organisations recognise social media to be a risk, there was still an absence of a social media policy in 65% of the organisations who participated in the study.

4.2.1 Policies

From the literature, the key challenge identified facing organisations in corporate social media communication has to do with developing adequate policies, implementing them and adhering to them. These policies should clearly define when and by whom these social media tools may be used in the working environment. Even more important would be what information would contravene the organisational policy and the consequences of this contravention. Brinkley (2014) suggests that corporate social media communication policies should include and provide for oversight, monitoring, strategy, role definition, users, communication and training.

The organisation's official use of social media as a marketing tool or mode of communication to stakeholders should also be addressed in the organisation's social media policies. An organisation's reluctance to invest and keep abreast of technology and the use of social media may have a detrimental effect on their competiveness (Aula *et al* 2010: Online). Employees who operate these systems and compile the information to be sent into the virtual world should similarly be well-informed of internal policy and legal pitfalls.

A survey conducted by Mushwana and Bezuidenhout (2014) on social media policy in South Africa further highlights the country's position with regard to such policies. Certain key findings revealed that:

- 48% of the respondents indicated that they do not have a social media policy, while 17% responded that they are not sure.
- Of the 35% that confirmed they do have a social media policy, only 60% responded that the policy was explained to employees to broaden their understanding of and commitment to its implementation.

The development of policies to control the risks resulting from the use of social media in the workplace is non-negotiable and should, like all other policies, be properly communicated and monitored.

4.2.2 Responses

There is no prescribed method of how organisations must respond to corporate social media communication crises. Our Social Times (2013:Online) outlines the following lessons organisations learned from their experience with Corporate Social Media Communication crises:

- Defending or justifying one's actions via the use of a corporate social media communication tool is not ideal.
- One's personal and organisation twitter accounts should be separated.
- One should respond quickly by way of an apology.
- Password security to prevent hacking is important.
- Employees should be educated about corporate social media communication policies.

Merrill *et al* (2011) further suggest five basic steps that management can implement to address corporate social media communication risks:

- conducting high-level assessments of the general social media activities in the organisation, looking for possible risks;

- identifying the relevant stakeholders or process owners who will be responsible for developing, executing and monitoring the organisation's social media strategy;
- developing a simplistic but detailed social media policy to be used as a guideline;
- work-shopping and addressing the risks of corporate social media communication with all employees of the organisation; and
- incorporating a social media agreement as part of the employee contract, this needs to be signed annually.

The implementation of social media policy should not be postponed until a crisis linked to the use of social media arises. Organisations and companies should learn from others' mistakes and implement clear and detailed policies.

4.3 Internal audit to advise management in risk identification and mitigation

The Committee of Sponsoring Organisations of the Treadway Commission (COSO) Framework (2013: Online) paved the way for internal auditing to expand its role to include risk management assurance in an organisation. This would imply that internal auditing should be involved in a consulting capacity in the design of internal controls. Due to the independent nature of the internal audit activity, this involvement would be limited to advice and feedback to management (Bogoslaw 2014: Online).

Internal auditing's role is governed by the International Standards for the Professional Practice (IPPF) of internal auditing. The IPPF Standard 2120 – Risk Management, states: "The internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes" (IIA 2012:Online). Further interpretation of this standard implies that internal auditing should assist management in identifying the risks and appropriate responses to mitigate those risks (IIA 2012:Online). The IIA further proposes that internal auditing be involved in enterprise-wide risk management by making available to management tools and techniques used by internal auditing to analyse risks and controls (IIA 2012: Online).

McCarthy and Krishna (2011:Online) are of the opinion that audit committees should ensure the involvement of internal auditing in corporate social media communication risks by focussing on issues such as whether management understands these risks, monitoring them and implementing policy to address them.

The many risks associated with the use of corporate social media communication in an organisation are frequently underestimated and misunderstood. It seems that management does not always take these risks seriously. Culp (2014:Online) refers to a recent survey, which investigated corporate social media risks and rewards. It revealed that 71% of executives surveyed believe that social media risks can be mitigated or avoided and a shocking 13% believed that their organisation did not have any considerable risks.

Brinkley (2014) quotes research conducted by Grant Thornton LLP in 2013, which reveals that social media governance is frequently neglected and even ignored. The study revealed that 59% of senior-level public and private organisations responded that their organisations did not conduct social media risk assessments (Brinkley 2014:68-69).

The task faced by internal auditing in educating management on the importance of mitigating risks associated with corporate social media communication, therefore, seems to be important. A study conducted by KPMG (2012:Online) revealed the importance of internal auditing in providing assurance when corporate social media communication is at risk.

In addition, Deloitte (2014:Online) suggests that internal auditing should assist management in the following key risk areas by:

- being involved in identifying potential crisis events that can lead to reputational risk and assisting management in developing and testing a contingency plan;
- benchmarking the organisation's existing policies and procedures against good practice and new legislative requirements by performing a gap assessment of the organisation's current policy framework;
- implementing data classification controls to prevent harmful information being shared;
- testing the controls in place to determine whether third-party service providers follow protocol at all times; and
- assessing the governance programme to ensure that it is competitive and ensures that communication of the policy is effective.

It is not only the employees' use of social media that causes potential risks, but also the way the organisation itself uses it to market themselves. The realisation of this risk generally results in reputational damage, legal liability and loss of production. It is thus evident that these risks need to be controlled since all will ultimately lead to financial loss of some kind, which might infringe on shareholder confidence (Deloitte 2014:Online).

Moreover, Culp (2014:Online) proposes that an organisation should approach the risks associated with corporate social media communication by addressing issues of governance, processes and systems. This could be a helpful tool for internal auditing when classifying risks. Hence, in the present study, the three areas of governance, processes and systems will be discussed, taking various literature reviews into account in order to serve as a guideline for internal auditing.

Governance

Management should ensure that structures and policies for the use of corporate social media communication in the organisation are comprehensive to encompass all corporate social media communication risks. Internal auditing should be part of these processes from the

onset. Bogoslaw (2014:Online) confirms that internal auditing is increasingly being asked to provide input while business strategies are initially being developed. Brinkley (2014) also suggests that corporate social media communication policies should include and provide for oversight, monitoring, strategy, role definition, users, communication and training.

Processes

Culp (2014:Online) suggests that organisations should, in consultation with internal auditing, develop and implement proactive risk-management processes that focus on the identification, reporting and monitoring of corporate social media communication risks.

Singleton (2012:Online) further proposes an auditing framework for corporate social media communication audits with two primary focus areas, namely: public image and operational effectiveness. The following points need to be considered when conducting audits:

- Information is sent into the social media cyberspace within seconds of an event taking place. In order to address the immediate risks to reputation/public image and productivity, internal auditing should ensure that measures are designed by management to control the rapid dissemination of information regarding the organisation.
- Preventative controls must be implemented to serve as an early warning system for potentially damaging information.
- Operational effectiveness of corporate social media communication risks should be audited the same way as any other information technology (IT) or systems audits.

Systems

Culp (2014:Online) suggests that management should invest in the resources and capabilities necessary to enable them to monitor risk associated with corporate social media communication. The following technology should be available:

- data mining software to enable management and auditors to access all corporate social media communication platforms;
- text analytic engines to recognise patterns in text;
- secure data storage technology; and
- dashboard monitoring to recognise vulnerabilities and risk.

Roath and Holcomb (2014:Online) focus on the internal controls in the IT environment. They emphasise the importance of the fact that the organisation should continually evaluate the adequacy of their IT and data security controls. Internal auditing could play a significant role in an organisation's understanding, monitoring and mitigation of IT related risks. A valid concern would be that the internal auditing might not have the necessary skills and competencies to do an in-depth assessment of risk in the IT environment. A low-level audit might provide management with a false sense of security. This apparent performance gap should be addressed by audit executives by identifying or recruiting talented and competent internal auditors. Brinkley (2014) agrees that the diverse communication tools used in the corporate environment involves a shift in the standard of internal auditing's approach to risks pertaining to reputation and compliance.

5 RESULTS AND DISCUSSION OF THE EMPIRICAL RESEARCH

In this section the results of the empirical research conducted through the distribution of questionnaires is presented. For questions one to four, only a short summary is provided because these questions provide the demographics of the population (refer to Annexure A).

The demographic data collected yielded the following:

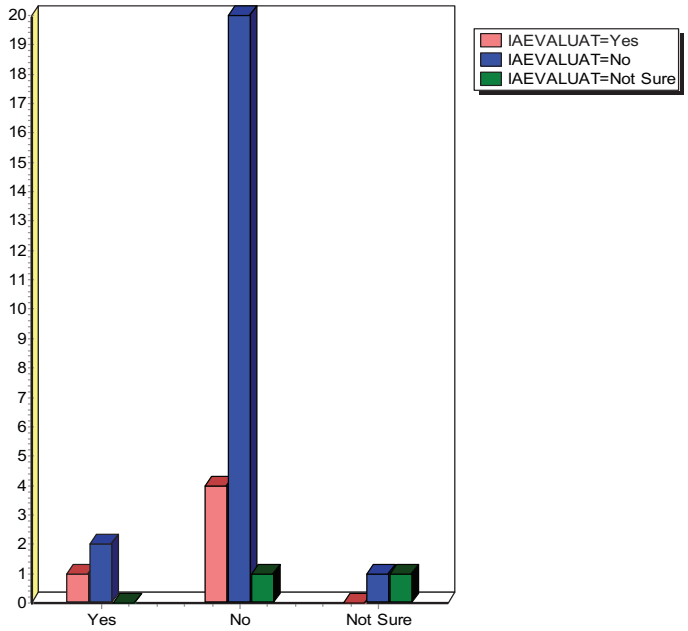
- The majority of the respondents (60%) were situated in the private sector.
- From the responses received, 76.67% of the respondents were from large organisations with at least 1 500 employees; 3.33% from medium-sized organisations with between 510 and 1500 employees; and the balance of 20% from "smaller" organisations with between 1 and 500 employees.
- A significant portion, 76.67%, of the respondents is in a position directly related to the internal audit environment. Only 23.33% of the respondents are not directly positioned in the internal audit environment.
- A significant portion (70%) of the respondents are qualified Certified Internal Auditors, which is a qualification directly related to the internal audit environment.

The results of questions three and four (the fact that the majority of the respondents are directly involved in the internal audit environment both by position (76.67%) and qualification (70%), provides a sense of comfort and justification regarding the results obtained for the rest of the questions (5–20), especially in terms of the quality of data obtained.

The rest of the results are discussed below and the necessary conclusions are drawn.

Table 2: The relationship between internal auditing evaluation and being trained to evaluate the effectiveness of corporate social media communication controls (Questions 5 & 6)

Was internal auditing trained to evaluate the effectiveness of controls?	Did internal auditing evaluate the effectiveness of controls?			Total
	Yes	No	Not Sure	
Yes	1	2	0	3
No	4	20	1	25
Not Sure	0	1	1	2
Total	5	23	2	30



A bivariate (cross-tabular) analysis was conducted to correlate the results of whether internal auditing evaluated the effectiveness of corporate social media communication controls and trained to do so. The results were intended to address the perception that the reason internal auditing did not evaluate the corporate social media communication controls is that they lacked the required training to do so. It is evident from the results that internal auditing is not evaluating the effectiveness of controls (76.66% – 23/30) and are not trained (83.33% – 25/30) to evaluate the effectiveness of corporate social media communication controls. The fact that the effectiveness of these controls is not tested by the majority of respondents is the primary concern and should be addressed as a priority. The assessment of controls is a basic auditing principle which does not require additional training. Subject-specific training should, however, be considered to provide background when developing the audit programme. A further attribute could also relate to the result (Table 6 below), which answers the question of whether corporate social media communication risks are included in the auditable activities and entities that constitutes the corporate internal audit universe.

Table 3: Development over the past 12 months in the use of corporate social media communication in organisations (Question 7)

Development over past 12 months	Number of responses	% of the number of responses received
Not at all	7	23.33%
Moderate	15	50%
Significant	8	26.67%
Total	**30**	**100%**

The majority of the respondents (76.67%) confirmed that the use of corporate social media communication developed extensively in their organisations over the last twelve months. This illustrates the significant increase and growth of corporate social media communication and its use in organisations, also in the literature review.

Table 4: The existence of a corporate social media communication policy (Question 8)

Existence of a policy	Number of responses	% of the number of responses received
Yes	14	46.67%
No	13	43.33%
Not sure	3	10%
Total	**30**	**100%**

More than half of the respondents (53.33%) indicated that they do not have (43.33%) or are not sure whether there is (10%) a corporate social media policy in their organisation. Only 46.67% indicated that a policy does exist in their organisation. With the increasing use of and the risks associated with corporate social media communication, one would have expected a higher percentage of organisations that had a policy to regulate the use and assist with the mitigation of the risks associated with corporate social media communication. Once again, this could pose a significant risk to the organisation.

Table 5: Who is responsible for monitoring the compliance with the corporate social media communication policy? (Question 9)

Who is responsible for monitoring the compliance with the corporate social media communication policy?	Number of responses	% of the number of responses received
IT department	10	33.33%
Risk manager	2	6.67%
Line management	10	33.33%
Executive management	0	0%
Internal audit	2	6.67%
Not applicable/not marked	6	20%
Total	**30**	**100%**

Although only 46.67% (14 of 30) indicated that a policy exists in their organisation (see table 4 above), only 20% of the respondents did not mark or indicate 'not applicable' on their forms when asked who is responsible for monitoring the compliance with the corporate social media communication policy in their organisations. What was encouraging to a certain extent was that only 6.67% indicated that it is the responsibility of internal auditing to monitor compliance with the corporate social media communication policy in their organisations. This indicates that these respondents realise that the monitoring of the implementation of an organisation's corporate social media communication policy is the responsibility of management, and not internal auditing.

Table 6: The identification of corporate social media communication risks in the risk universe of the organisation (Question 10)

Risks identified in risk universe	Number of responses	% of the number of responses received
Yes	14	46.67%
No	12	40%
Not sure	4	13.33%
Total	**30**	**100%**

A disappointing 46.67% responded that the risks associated with corporate social media communication have been included in the organisation's risk universe. Based on the negative consequences these risks can have on organisations and the increasing growth in the use of corporate social media communication as outlined in the literature review and case studies researched, one would have expected the percentage to be significantly higher. Forty per cent responded that these risks have not been included, which may also be a cause for concern because this implies that these organisations may not even be aware of their risks with regard to corporate social media. Mushwana and Bezuidenhout (2014) argue that management's perception of the risks; the identification and designation of a risk owner and the inclusion of social media risk in the risk universe of organisations are the first three steps to consider when addressing the risks of corporate social media communication in organisations. Juergens (2013: Online) points out that there seems to be a huge oversight by management in that they do not realise or they overlook the valuable resource they have in internal auditing who can assist them with managing and mitigating the risks and challenges to which they are exposed by corporate social media communication.

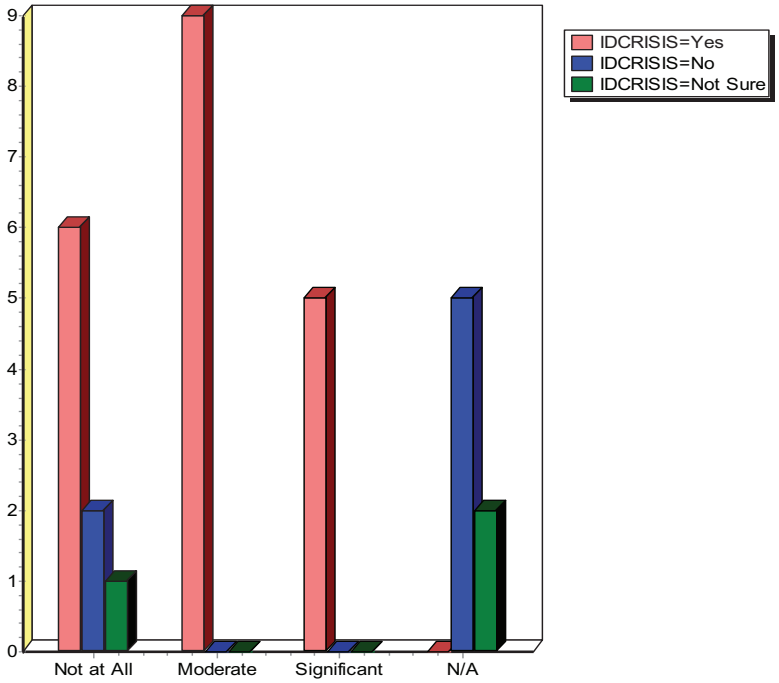
Table 7: Identify potential crisis events pertaining to brand and reputational damage (Question 11)

Potential crisis events identified pertaining to brand and reputational damage	Number of responses	% of the number of responses received
Yes	20	66.67%
No	7	23.33%
Not sure	3	10%
Total	**30**	**100%**

An overwhelming 66.67% of the respondents indicated that they have identified potential crisis events related to brand and reputational risk. This supports the 66.67% that identified brand and reputational risk as the most significant for organisations (see table 9 below) and the reviewed case studies that revealed as the most prominent risk (see table 1 above). It is suggested by Deloitte (2014:Online) that there is a possibility to expand the role of an organisation's internal audit activity to include involvement in assessing and identifying risks pertaining to corporate social media communication, taking into account the harm an organisation's reputation can suffer.

Table 8: The relationship between the identification of crisis events pertaining to brand and reputational damage and the extent to which internal auditing was involved (Questions 11 & 12)

To which extent was internal auditing involved?	Did the organisation identify potential crisis events pertaining to brand and reputational damage?			Total
	Yes	No	Not Sure	
Not at all	6	2	1	9
Moderate	9	0	0	9
Significant	5	0	0	5
Not Applicable	0	5	2	7
Total	20	7	3	30



A bivariate (cross-tabular) analysis was conducted to correlate the results about the extent to which internal auditing was involved in the identification of crisis events pertaining to brand and reputational damage. The results were intended to address the perception that internal auditing does not do enough to assist management in addressing one of the most significant risks identified by organisations (see table 9 below). Twenty (66.67%) of the respondents identified potential crisis events pertaining to brand and reputational damage, while only five (16.67%) stated that internal auditing was significantly involved in the organisation's process of identifying potential crisis events relating to brand and reputational damage.

The pro-active involvement of internal auditing in identifying potential crisis events relating to brand and reputational risks would not only enhance an organisation's governance processes but could also save the organisation substantial financial losses.

Table 9: The highest-ranking social media risk (Question 13)

Highest-ranking risk	Number of responses	% of the number of responses received
Brand and reputation	20	66.67%
Data security	7	23.33%
Regulatory compliance	1	3.33%
Data leakage	1	3.33%
Viruses and malware	1	3.33%
Total	**30**	**100%**

An overwhelming 66.67% of the respondents indicated brand and reputational risk as the most significant risk. This is supported by the literature. The case studies reviewed in section 4.1 provided similar results. Only 23.33% (a significant drop) of the respondents named data security as the second highest risk. The results of regulatory compliance, data leakage and viruses and malware were somewhat unexpected as the world is operating at a technologically advanced level, which creates the expectation that IT-related issues would come to the fore.

Table 10: Who plays the most significant role in corporate social media communication risk assessment in the organisation? (Question 14)

Who plays the most significant role in corporate social media communication risk assessment in the organisation?	Number of responses	% of the number of responses received
IT department	6	20%
Risk manager	10	33.33%
Line management	6	20%
Executive management	3	10%
Internal audit	2	6.67%
Not applicable/not marked	3	10%
Total	**30**	**100%**

Only 10% of the respondents did not mark or indicate 'not applicable' on their forms when asked who plays the most significant role in corporate social media communication risk assessment in the organisation. A total of 83.33% indicated that their own management plays the most significant role. It is reassuring that the respondents realise that it is not internal auditing that should be at the forefront, but that management should drive the corporate social media communication risk assessment in their organisations.

Table 11: Inclusion of corporate social media communication risks in the internal audit universe (Question 15)

Risks included in the internal audit universe	Number of responses	% of the number of responses received
Yes	10	33.33%
No	15	50%
Not Sure	5	16.67%
Total	**30**	**100%**

A mere 33.33% confirmed that the risks associated with corporate social media communication are included in the internal audit universe. This could be as a result of three factors: firstly, an overwhelming 76.66% of the respondents indicated that internal auditing does not evaluate the effectiveness of controls (see table 2 above); secondly, 83.33% stated that internal auditing is not trained to evaluate the effectiveness of corporate social media communication controls (see table 2 above); and thirdly, a disappointing 46.67% confirmed that the risks associated with corporate social media communication have not been included in the organisation's risk universe (see table 6 above).

Table 12: Has internal auditing conducted a corporate social media communication review during the past three years? (Question 16)

Review done in the past three years?	Number of responses	% of the number of responses received
Yes	4	13.33%
No	23	76.67%
Not Sure	3	10%
Total	**30**	**100%**

The table above illustrates that 76.67% of the respondents confirmed that a corporate social media communication review was not conducted during the last three years. A mere 13.33% responded positively to a review having been conducted. These results confirm the perception that internal auditing still has a long way to go in terms of their involvement in mitigating the risks associated with corporate social media communication. Tracking internal auditing's improvement in attending to this matter could be an area for future research.

Table 13: To what extent did the internal auditing review add value to your organisation? (Question 17)

To what extent did the internal auditing review add value to your organisation?	Number of responses	% of the number of responses received
Low	1	3.33%
Moderate	3	10%
High	0	0%
Not Sure	2	6.67%
Not Applicable	24	80%
Total	**30**	**100%**

Only 13.33% of the respondents indicated that internal auditing added some value when they conducted a corporate social media communication review in the organisation during the past three years.

A significant percentage (80%) responded with 'not applicable', and 6.67% said that they are unsure whether any value was added. Consistent with the IIA SA standards (IIA 2012:Online), it appears from this result that the internal audit activity is not fulfilling its mandate of adding value to corporate social media communication. This also confirms the perception that internal auditing can do much more and should step-up in their role of assisting management to mitigate the risks associated with corporate social media communication.

Table 14: The extent to which internal auditing provided input to ensure secure information technology and data systems (Question 18)

Internal auditing input provided into information technology and data systems	Number of responses	% of the number of responses received
Not at all	5	16.67%
Moderate	15	50%
Significant	9	30%
No response	1	3.33%
Total	**30**	**100%**

Only 20% responded negatively, which indicates that internal auditing's opinions matter to the organisation to secure data and information. This result also supports the "lower" rating identified for the data leakage risk as identified by organisations (see table 9 above).

Table 15: Did internal auditing assess and comment on the effectiveness of the organisations' governance structures? (Question 19)

Did internal auditing assess and comment on the effectiveness of the organisations' governance structures?	Number of responses	% of the number of responses received
Yes	20	66.67%
No	9	30%
Not sure	1	3.33%
Total	**30**	**100%**

The internal audit activity provides assurance to management and the audit committee on three basic areas, namely: internal controls, risk management and governance of the organisations (IIA 2012: Online). It is encouraging to note that the majority (66.67%) of the respondents indicated that internal auditing assessed and commented on the effectiveness of their organisations' governance structures. Regardless of the aforementioned, it is a cause for concern that 30% of the respondents have a negative opinion of internal auditing's involvement in governance. This indicates that there is room for improvement.

Table 16: Out-sourced corporate social media communication contracts reviewed by internal auditing (Question 20)

Internal auditing review of out-sourced corporate social media communication contracts	Number of responses	% of the number of responses received
Yes	0	0%
No	14	46.67%
Not sure	4	13.33%
Not marked	12	40%
Total	**30**	**100%**

Although no positive response was received, this result can most likely be attributed to the high percentage (40%) that did not respond to the question. This in itself might be an area of concern as it implies that internal auditing was not given the opportunity to provide any assurance in respect of compliance to contractual agreements concerning social media. This has the potential to evolve into more risks being faced by the organisation.

6 CONCLUSION

The aim of this study was two-fold: firstly, to determine, through review of case studies, the various risks, effects and challenges that corporate social media communication poses for organisations. Secondly, the study aimed to explore the extent of the involvement (i.e. the role) of internal auditing in assisting the management of organisations to evaluate and mitigate the risks that corporate social media communication poses.

Corporate social media communication, if not managed properly, can lead to legal, financial and reputational risks for organisations, as outlined by Ployhart (2014). With a majority of 76.67% of respondents confirming the significant and moderate development of corporate social media communication in their organisations in the last twelve months, the study revealed that management needs to attend to

corporate social media communication and, therefore, cannot ignore the risks associated with it. Although 46.67% responded that the risks associated with corporate social media communication have been included in the organisation's risk universe, the organisation did not have a corporate social media communication policy. With the phenomenal growth of corporate social media communication and the risks it poses as outlined in the literature review, one would have expected these percentages to be higher.

The chief audit executives at organisations should review their commitment to management in light of the low percentage (66.67% in total) that confirmed either that corporate social media communication risks are not included in the internal audit universe (50%) or that they are not sure (16.67%) whether or not this was the case. To make matters worse, the study revealed alarming results of 76.66% and 83.33% indicating that internal auditing was not evaluating and not trained to evaluate the effectiveness of corporate social media communication controls. These results highlight the need for chief audit executives and internal audit management to re-examine the competency of the internal audit members to address these risks and be in a position to add value to the organisation.

Lastly, the 76.67% response that internal auditing did not conduct any corporate social media communication reviews during the past three years is evident that internal auditing might not be doing enough. It is time to step-up and assists management in mitigating the risks associated with corporate social media communication.

7 RECOMMENDATIONS

One of the interventions management can put in place to address the corporate social media communication risks and challenges they face is the development and implementation of corporate social media communication policies as well as the method and timing of its responses to these crises.

Based on internal auditors' knowledge and experience of risk management, they should be actively involved in providing advice in the design of structures, policies, risk management processes and security systems pertaining to social networking in the workplace.

The responsibility of internal auditing with regard to risks associated with corporate social media communication is thus, as with all other risks, non-negotiable. The internal audit activity can assist management in mitigating the risks associated with corporate social media communication by:

- being involved from the onset in the design and execution of internal controls;
- identifying and analysing risks and their appropriate responses; and
- educating management about the importance of mitigating risks associated with corporate social media communication.

REFERENCES

Aguenza, B. & Puad Mat Som, A. 2012. A conceptual analysis of social networking and its impact on employee productivity. *IOSR Journal of Business and Management*, 1(2):48-52. [Online]. http://www.iosrjournals.org (Accessed: 17 September 2015).

Anderson, G., Varne, R.M., Warren, P.D., Czerwinski, J.M. & Andolina, E.G. 2011. *Managing Third-Party Relationship Risk*. [Online]. http://www.crowehorwath.com (Accessed: 27 August 2014).

Aula, P., Laaksonen, S. & Neiglick, S. 2010. *Reputational Risks and the Rising of Digital Publicity*. [Online]. http://www.helsinki.fi/crc/en (Accessed: 27 August 2014).

Babbie, E.R. 2009. *The Practice of Social Research.* 12th edition. Belmont: Wadsworth.

Baker, D., Buoni, N., Fee, M. & Vitale, C. 2011. *Social Networking and Its Effects on Companies and Their Employees.* Aston: Neumann University.

Berman, J. 2014. *The Three Essential Warren Buffet Quotes To Live By.* [Online]. http://www.forbes.com/sites (Accessed: 17 September 2015).

Bogoslaw, D. 2014. *Internal Audit Getting in Early on Strategic Planning*. [Online]. http://www.corporatesecretary.com/articles/risk-management-d-o-liability/12698/internal-audit-getting-early-strategic-planning/ (Accessed: 10 March 2015).

Brogan, C. 2010. *Social media 101: tactics and tips to develop your business online.* Hoboken: John Wiley and Sons.

Brinkley, M. 2014. Governance perspectives. *Internal Auditor*, April:68-69.

Business Dictionary. n.d. *Reputational Risk.* [Online]. http://www.businessdictionary.com/definition/reputation-risk.html (Accessed: 27 August 2014).

Business Dictionary. 2016. *Corporation.* [Online]. http://www.businessdictionary.com/definition/corporation.html (Accessed: 16 September 2016).

Cambridge Dictionaries Online. 2014a. *Third Party Risk*. [Online]. http://www.dictionary.cambridge.org (Accessed: 4 September 2014).

Cambridge Dictionaries Online. 2014b. *Productivity Risk*. [Online]. http://www.dictionary.cambridge.org (Accessed: 4 September 2014).

Castellan, C.M. 2010. Quantitative and qualitative research: A view for clarity. *International Journal of Education*, 2(2):7. [Online]. http://www.macrothink.org/ije. (Accessed: 16 September 2015).

Cavico, F.J., Mujtaba, B.G., Muffler, S.C. & Samuel, M. 2013. Social media and employment-at-will: Tort law and practical considerations for employees, managers and organizations. *New Media and Mass Communication*, (11):25-41.

COSO 2013. *Internal control framework*. [Online]. http://www.coso.org/documents/990025P_Executive_Summary_final_may20_e.pdf. (Accessed 5 September 2015).

Creswell, J.W. 2003. *Research Design: Qualitative, Quantitative and Mixed Methods Approaches.* Thousand Oaks: Sage.

Culp, S. 2014. *A Comprehensive Approach to Managing Social Media Risk and Compliance.* [Online]. http://www.accenture.com/sitecollectiondocuments/financial-services/accenture-comprehensive-approach-managing-social-media-risk-compliance (Accessed: 12 March 2015).

Deloitte & Forbes Insights. 2013. *Aftershock: Adjusting to the new World of Risk Management*. [Online]. http://www2.deloitte.com/us/en/pages/governance-risk-and-compliance/articles/aftershock.html (Accessed: 4 September 2015).

Deloitte. 2009. *Social networking and reputational risk in the workplace: Deloitte LLP 2009 ethics & workplace survey results.* [Online]. http://www.slideshare.net/PingElizabeth/deloitte-2009-ethics-workplace-survey. (Accessed: 4 September 2015).

Deloitte. 2014. *Social Media Risks Create an Expanded Role for Internal Audit*. [Online]. http://www.deloitte.wsj.com (Accessed: 4 September 2014).

Enlightenme n.d. *What Is Compliance Risk?* [Online]. http://www.enlightenme.com/compliance-risk/. (Accessed: 21 October 2015).

Ferreira, A. & Du Plessis, T. 2009. Effect of online social networking on employee productivity. *SA Journal of Information Management*, 11(1):2-6.

Fleming, M.B. & Miles, A.K. 2012. Punishing employees for using social media outside the scope of their employment: What are the potential legal repercussions to the private employer? *ALBS Journal of Employment and Labour Law*, 13:1-22.

Gordon, P. 2007. *Data Leakage: Threats and Mitigation.* [Online]. https://www.sans.org/reading-room/whitepapers/awareness/data-leakage-threats-mitigation-1931 (Accessed: 4 September 2015).

Greenwald, J. 2009. Employees' social networking raises employers' liability risk. *Business Insurance*, 19 July. [Online]. https://www.businessinsurance.com/article/20090719/ISSUE01/307199966 (Accessed: 12 March 2015).

Hudson, S.C. & Roberts, K.K. 2012. Drafting and implementing an effective social media policy. *Texas Wesleyan Law Review*, 18:767-794.

Institute of Internal Auditors. 2012. *International standards for the professional practice of internal auditing (Standards) – Revised October 2012.* [Online]. https://www.na.theiia.org/standards-guidance/Public%20Documents/IPPF%202013%20English.pdf (Accessed: 27 August 2015).

Juergens, M. 2013. *Social media risks create an expanded role for internal audit.* [Online]. http://www.deloitte.wsj.com/cfo/2013/08/15/social-media-risks-create-an-expanded-role-for-internal-audit (Accessed: 4 September 2015).

Kelsey, M.D. & Matossian, M. 2004. Compliance Risk: Ensuring the risk taken is the Risk Intended. *AB Bank Compliance*, May/June:6. [Online]. http://www.aba.com/Compliance/ (Accessed: 18 September 2015).

KPMG. 2012. *Social Media Internal Audit's response*. [Online]. https://www.kpmg.com/BE/en/IssuesAndInsights/ArticlesPublications/Documents/Social%20Media_ITIA's%20response.pdf (Accessed: 12 March 2015).

KPMG. 2014. *Financial Services Regulatory Point of View: The New Third-Party Oversight Framework: Trust but Verify.* [Online]. http://www.kpmg.com. (Accessed: 17 September 2015).

Magcaba, S. 2013. *FHM 'rape comment' employees fired.* [Online]. http://www.enca.com/south-africa/fhm-employees-fired (Accessed: 4 September 2015).

McCarthy, M.P. & Krishna, S. 2011. *Social Media: Time for a Governance Framework.* [Online]. https://www.kpmg.com/US/en/IssuesAndInsights/ArticlesPublications/Documents/social-media-time-for-governance.pdf (Accessed: 4 September 2015).

McCorkindale, T. & DiStaso, M.W. 2013. The Power of Social Media and Its Influence on Corporate Reputation. In C.E. Carroll (ed.). *The Handbook of Communication and Corporate Reputation*, pp. 496-508. Oxford: Blackwell Publishing.

Media News. 2012. *Managing Online Reputational Risk.* [Online]. http://www.bizcommunity.com/Article/196/15/74767.html (Accessed: 4 September 2014).

Merrill, T., Latham, K., Santalesa, R. & Navetta, D. 2011. *Social media: The business benefits may be enormous, but can the risks – reputational, legal, operational – be mitigated.* Zurich: ACE.

Mushwana, G. & Bezuidenhout, H. 2014. Social media policy in South Africa. *The Southern African Journal of Accountability and Auditing Research.* 16:63-74.

Mybroadband. 2014. *FNB Twitter "joke" causes online storm*. [Online]. http://www.mybroadband.co.za/news/internet/100964-fnb-twitter-joke-goes-wrong.html. (Accessed: 4 September 2014).

Osborne, C. 2011. *Apple's internal employee social media policies leaked*. [Online]. http:// www.zdnet.com/blog/igeneration (Accessed: 4 September 2015).

Our Social Times. 2013. *6 Examples of social media crises: What we can learn*. [Online]. http://www.oursocialtimes.com/6-examples-of-social-media-crises-what-can-we-learn. (Accessed: 5 September 2015].

Ployhart, R.E. 2014. *Social Media in the Workplace: Issues and Strategic Questions.* Alexandria: SHRM Foundation.

Recalde, M.E. 2010. *The Need For a Social Media Policy.* [Online]. http://www.sheehan.com (Accessed: 4 September 2015).

Roath, D. & Holcomb, C. 2014. *Internal Audit Should Play Bigger Role in IT*. [Online]. http://www.2.cfo.com/risk-management/2014/10/internal-audit-play-bigger-role/ (Accessed: 10 March 2015).

Singleton, T.W. 2012. *What Every IT Auditor Should Know About Auditing Social Media.* [Online]. http://www.isaca.org/Journal/archives/2012/Volume-5/Pages/What-Every-IT-Auditor-Should-Know-About-Auditing-Social-Media.aspx. (Accessed: 10 March 2015).

Smith, M.J. 1988. *Contemporary Communication Research Methods*. Belmont: Wadsworth Publishing.

Walter, I. 2006. *Reputational Risk and Conflicts of Interest in Banking and Finance: The Evidence So Far*. [Online]. http://www.ssrn.com/abstract=952682 (Accessed: 18 September 2015).

Wellman, J.C. & Kruger, S.J. 2001. *Research Methodology*. Cape Town: Oxford University Press.

Wilson, J. 2009. Social networking: The business case. *Engineering & Technology*, 4(10):54-56.

Zarella, D. 2010. *The social media marketing book.* North Sebastopol: O'Reilly Media.

Zurich. 2008. *Strategies for managing information security risks*. [Online]. https://www.zurich.com (Accessed: 17 September 2015).

ANNEXURE A

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

Department of Auditing
Tel: (012) 420 - 4427
Fax :(012) 420 - 4547
http://www.up.ac.za

Letter of Introduction and Informed Consent

Department of Auditing

Title of the Study: Risks faced with Corporate Social Media Communication –

Time for Internal Auditing to step-up

Research conducted by:

Mrs SC Green (13336020)
Cell: 082 300 9262

Dear Participant

You are invited to participate in an academic research study conducted by Sharon Charmaine Green, Masters Student from the Department of Auditing at the University of Pretoria. The purpose of the study is to investigate the role of Internal Auditing in providing assistance to management in mitigating the risks associated with Corporate Social Media Communication.

Please note the following:

- This is an anonymous survey as your name will not appear on the questionnaire. The answers you give will be treated as strictly confidential as you cannot be identified in person based on the answers you give.
- Your participation in this study is very important to us. You may, however, choose not to participate and you may also stop participating at any time without any negative consequences.
- Please answer the questions in the attached questionnaire as completely and honestly as possible. This should not take more than 15 minutes of your time.
- The results of the study will be used for academic purposes only and may be published in an academic journal. We will provide you with a summary of our findings on request.
- Please contact the study leader, Professor H. de Jager, contact number 012 420 6955, herman.dejager@up.ac.za if you have any questions or comments regarding the study.

Please tick the applicable box to indicate that:

- You have read and understand the information provided above.

  ☐ Yes ☐ No

- You give your consent to participate in the study on a voluntary basis.

  ☐ Yes ☐ No

Questionnaire - Risks faced with Corporate Social Media Communication –

Time for Internal Audit to step-up

The purpose of the study is to investigate the role of Internal Auditing in providing assistance to management in mitigating the risks associated with Corporate Social Media Communication.

Once you have completed the questionnaire, please submit to:

Sharon Green

Email address:GreenS@saps.gov.za

#	Question
1	Which sector do you work in? ☐ Public ☐ Private
2	What is the size of your organisation in respect of the number of employees? ☐ 1 - 100 ☐ 101 - 500 ☐ 501 – 1500 (Medium) ☐ 1501+
3	What qualifications/designation (highest) do you hold? ☐ CA (SA) ☐ Master's Degree ☐ Honours Degree ☐ CIA ☐ B.Com Degree ☐ Other
4	What is your position in the organisation? ☐ CAE ☐ Internal Audit Manager ☐ Internal Audit Supervisor ☐ Internal Auditor ☐ Other
5	Did Internal Audit evaluate the effectiveness of Social Media Communication controls? ☐ Yes ☐ No ☐ Not sure
6	Was Internal Audit trained to evaluate the effectiveness of Social Media Communication controls? ☐ Yes ☐ No ☐ Not sure
7	How did corporate use of Social Media Communication develop in your organisation over the past 12 months? ☐ Not at all ☐ Moderate ☐ Significant
8	Does your organisation have a Corporate Social Media Communication policy in place? ☐ Yes ☐ No ☐ Not sure
9	Who is responsible to monitor the compliance to the Social Media Communication policy? ☐ IT Department ☐ Risk Manager ☐ Line Management ☐ Executive Management ☐ Internal Audit
10	Have risks associated with Corporate Social Media Communication been identified in the risk universe of your organisation? ☐ Yes ☐ No ☐ Not sure
11	Did the organisation identify potential crisis events pertaining to brand and reputational damage? ☐ Yes ☐ No ☐ Not sure
12	If you answered 'yes' to Q11 above, to what extent was Internal Audit involved? ☐ Not at all ☐ Moderate ☐ Significant

13	Which social media risks are rated the highest risk in the organisation? ☐ Brand and Reputatio ☐ Data Security ☐ Regulatory Compliance ☐ Data leakage ☐ Viruses and Malware
14	Who plays the most significant role in social media risk assessment in the organisation? ☐ IT department ☐ Risk Manager ☐ Line Management ☐ Executive Management ☐ Internal Audit
15	Have you included Corporate Social Media Communication risks in your Internal Audit universe? ☐ Yes ☐ No ☐ Not sure
16	Have the Internal Audit Activity conducted a Corporate Social Media Communication audit review in the past three years? ☐ Yes ☐ No ☐ Not sure
17	If you answered 'yes' to Q16 above: To what extent did the internal audit review add value to your organisation? ☒ Low ☐ Moderate ☐ High ☐ Not sure
18	To what extent did Internal Audit provide input to ensure secure information technology and data systems? ☐ Not at all ☐ Moderate ☐ Significant
19	Did Internal Audit assess and comment on the effectiveness of the organisations' governance structures? ☐ Yes ☐ No ☐ Not sure
20	If your organisations' social media was outsourced, did Internal Audit review the contracts to ensure that the contractual procedures were followed? ☐ Yes ☐ No ☐ Not sure

The Southern African Journal of Accountability and Auditing Research

Evolving Research

Measuring corporate governance in South Africa: Developments, concerns and suggestions

N Mans-Kemp — Department of Business Management, Stellenbosch University

P Erasmus — Department of Business Management, Stellenbosch University

S Viviers — Department of Business Management, Stellenbosch University

ABSTRACT

A large and increasing number of corporate governance guidelines have emerged on the African continent over the last two decades. Limited research has, however, been conducted to comprehensively assess the corporate governance policies and practices of listed African companies. The researchers hence compiled a unique corporate governance database for 230 companies that were listed on the Johannesburg Stock Exchange over a nine year study period. Attention was given to both disclosure and acceptability dimensions for nine corporate governance categories. Positive developments were noted for the director-related categories, while reporting on sustainability and corporate culture aspects showed less improvement. A number of unacceptable practices were also observed. Enhanced training for directors, managers and auditors is recommended to improve their understanding of their roles and responsibilities. Furthermore, the media can encourage more active corporate governance-related dialogue by reporting on inefficiencies and highlighting positive developments.

Key words

Corporate governance; South Africa; disclosure; accountability

1 INTRODUCTION

Since the 1990s, a considerable number of corporate governance codes, guidelines and reports were issued globally, illustrating the relevance thereof to policymakers and practitioners (John & Makhija 2011). The majority of these reports guided the behaviour of directors. The guidelines were often followed strictly in an attempt 'to tick the compliance boxes'. However, South African legal advisor Johan Myburgh warned that corporate governance is not merely a matter of what is right or wrong - it is more nuanced than that (Corporate Governance Framework Research Institute 2016:Online).

Corporate governance includes two dimensions, namely 'doing the right things' (disclosure) and 'doing things right' (acceptability) (Van den Berghe & De Ridder 1999). Accordingly, researchers should give attention to both corporate governance disclosure (i.e. information provided on a listed company's corporate governance practices) and acceptability (whether the disclosed practices were in line with the prescribed corporate governance guidelines).

Extensive corporate governance research was conducted over the last two decades (1995-2015), primarily in developed countries. A review of extant corporate governance literature revealed that researchers employed diverse measurement instruments that were based on country-specific guidelines. While the majority of researchers focused on the composition of listed companies' directorates, some authors (such as Ntim, Opong & Danbolt 2012; Mangena & Chamisa 2008; Moloi 2008; Abdo & Fisher 2007) used comprehensive measuring instruments. The latter authors evaluated the disclosure of corporate governance practices based on information provided in the annual reports of large firms that were listed on the Johannesburg Stock Exchange (JSE) during the 2000s. Small and delisted firms were typically excluded from their samples.

Previous authors had failed to address the acceptability dimension when assessing the corporate governance practices of JSE-listed firms. Given that the corporate governance practices of local public companies were guided by the King II Report for almost a decade, the authors set out to investigate

the corporate governance reporting of a sample of JSE-listed companies over the period 2002 to 2010. In contrast to previous local authors who focused on corporate governance disclosure, consideration was given to both disclosure and acceptability criteria whilst analysing data pertaining to nine corporate governance categories. For this purpose, content analysis was conducted on the 230 sample firms' annual reports. The sample included small, medium and large companies based on market capitalisation. Delisted companies were included to limit survivorship bias.

The objectives of this article were threefold. Firstly, to compile a unique corporate governance database based on the reported corporate governance practices of selected JSE-listed firms during the period that the King II Report was employed. The available local corporate governance measuring instruments hence had to be reviewed to select an appropriate measure for the purpose of this study. Secondly, to identify corporate governance concerns whilst employing the observational content analysis technique. Thirdly, to provide suggestions to address some of the concerns related to the King II-regime. Reference was also made to whether these aspects were addressed in the King III Report.

The remainder of the article is structured as follows: global and local corporate governance developments are examined, followed by an explanation of local corporate governance measuring instruments. Thereafter, the methodology and research findings are discussed. Finally, pertinent conclusions, limitations and recommendations are presented.

2 GLOBAL AND LOCAL CORPORATE GOVERNANCE DEVELOPMENTS

A review of the literature suggests that there are four main corporate governance systems, namely: The Germanic, Latin, Japanese and Anglo-Saxon systems (Weimer & Pape 1999). The prominent Anglo-Saxon system centres on shareholders' wealth maximisation. Traditionally, the primary objective of managers is considered to be the maximisation of shareholders' wealth, since they are the owners of a company. In line with Freeman's (1984) argument that the interests of various stakeholders, including shareowners and employees should be considered, shareholders' wealth maximisation might be better achieved with the co-operation of key stakeholders (Jones & Felps 2013).

Corporate governance guidelines that were published in the United States of America (USA) and the United Kingdom (UK) were based on the Anglo-Saxon system. The Cadbury Report was published in 1992 to provide corporate governance guidelines to companies operating in the UK. The downfall of corporate giants such as Enron and WorldCom sharply focussed the world's attention on the possible abuse of power by corporate agents. In 2002, shortly after the collapse of these two companies, the Sarbanes-Oxley Act was signed into law in the USA (Northrup 2006:5).

Despite a slow start in the 1990s, the publication of corporate governance codes grew rapidly worldwide. In 2003, 35 countries had at least one code (European Corporate Governance Institute (ECGI) 2013:Online). By the middle of 2015, approximately 420 corporate governance codes existed (ECGI 2015:Online). Although the majority of these codes were published in developed countries, the publication of African corporate governance guidelines increased considerably.

Nigeria and South Africa published the most corporate governance reports on the African continent over the last 20 years (1994-2014). Several corporate scandals in Nigeria necessitated the publication of corporate governance guidelines (Boubaker & Nguyen 2014). Since 2003, five corporate governance publications were released in this country. Three King Reports on corporate governance were published since 1994 in South Africa (ECGI 2015:Online).

Before 1994, the Apartheid regime resulted in considerable concentration of corporate ownership in South Africa. A few large firms, specifically mines controlled by Anglo-American families, such as the Oppenheimers, dominated the local economy. Furthermore, political and economic sanctions limited international trade and investment opportunities. The Apartheid government hence used an active industrial policy based on the development of state-owned enterprises. Selected private and public institutions largely controlled corporate finance. Although institutional investors held board seats in influential companies, they did not effectively monitor corporate operations *per se* (Habbard 2010:Online).

Following the end of the Apartheid regime in 1994, several corporate governance reforms ensued in South Africa. Pyramid structures were prohibited and corporate self-regulation started to play an important role in shaping the local corporate governance landscape.

2.1 The King Reports on corporate governance

The first King Report primarily provided standards of conduct to the directors of JSE-listed firms in 1994. In line with the Cadbury Report that centred on the accountability of boards to shareholders, the directorate is regarded as the focal point of the local corporate governance system. The country's colonial history possibly had an influence on the adoption of UK-related corporate law and corporate governance guidelines. Board-related aspects, such as meeting frequency and executive remuneration received considerable attention (Habbard 2010:Online; Institute of Directors in Southern Africa (IoDSA) 1994).

The publication of the first King Report evoked unprecedented interest in corporate governance locally and globally. Adherence to this voluntary report was practiced on a 'comply or explain' basis. JSE-listed companies hence had to disclose in their annual reports whether they complied with the King II guidelines or explain their non-compliance (Malherbe & Segal 2001). Legislation and global corporate governance-related developments necessitated the publication of the King II Report in 2002. This report provided guidelines on, *inter alia*, stakeholder relationships and the so-called triple bottom line

reporting related to a company's economic, environmental and social activities (IoDSA 2002).

The third King Report, which was published in 2009, recommended that JSE-listed companies should publish integrated reports, reflecting their financial and sustainability-related performance (IoDSA 2009). As with the previous two King Reports, the JSE adapted its listing requirements accordingly. Consequently, all JSE-listed firms have been required to publish integrated reports since 2011 (Pretorius 2011). In contrast to the first two King Reports, the King III Report follows an 'apply or explain' approach. Focus is accordingly placed on how JSE-listed companies apply the King III principles in practice (IoDSA 2009). The King IV Report is forthcoming by the end of 2016.

South African principle officers of pension funds and asset managers regard corporate governance as quite important when making investment decisions (Eccles, De Jongh, Nicholls, Sinclair & Walker 2007:Online). This tendency could be ascribed to the well-developed, stakeholder-inclusive local corporate governance framework. Investors require detailed information to make informed decisions. Unfortunately, there was a lack of information on the corporate governance practices of firms operating in emerging countries, including South Africa, in the 2000s (Organisation for Economic Co-operation and Development 2007:Online). Furthermore, certain local firms tend to follow a minimalistic corporate governance compliance and reporting approach. The well-known South African shareholder activist, Theo Botha has often criticised JSE-listed firms in the local media for failing to comply with the King II Report. He has attributed companies' behaviour to the voluntary nature of this report (Carte 2009:Online).

3 CORPORATE GOVERNANCE MEASURING INSTRUMENTS

When this study commenced, there was a lack of standardised, detailed corporate governance data for firms that were listed on the JSE during the King II-regime. Consequently, the researchers had to identify an appropriate research instrument to evaluate the corporate governance practices as indicated in their annual reports. Table 1 presents a summary of the measuring instruments that were developed by local researchers to compile corporate governance scores (CGSs) for firms listed on the JSE main board.

Table 1: Corporate governance measuring instruments employed by local researchers

Instrument and author(s)	Aspects included	Sample and time frame	Findings
G-Score (Abdo & Fisher 2007)	Specific recommendations of the King II Report and the Standard and Poor's 1997 International corporate governance score index. Consists of 29 disclosure factors for seven categories (board effectiveness, remuneration, audit and accounting, internal audit, risk management, sustainability and ethics).	97 JSE-listed firms; 2003 and 2005	Corporate governance disclosure standards varied widely amongst firms. Poor governance standards were identified within certain JSE-sectors. Investors placed a premium on sample firms that was well governed.
Research checklist (Moloi 2008)	Seven categories (board and directors, risk management and internal controls, internal audit, integrated sustainability reporting, accounting and auditing, relation and communication with company shareholders, company's code of ethics) based on selected King II recommendations and the Corporate Laws Amendment Act (No. 24 of 2006).	Top 40 JSE-listed firms; 2006	The majority of the firms adhered to good corporate governance disclosure practices. There were areas where the non-disclosure of information was prevalent, e.g. the selection of external auditors and whistle blowing.
Corporate governance index (Mangena & Chamisa 2008)	Six factors (board size, board composition, chairperson and chief executive officer role duality, audit committee presence, directors' share ownership, block share ownership) based on the King I and II recommendations.	81 firms that were suspended from the JSE; 1999-2005	The likelihood of suspension was higher for firms with a smaller proportion of non-executives (NEDs), without an audit committee and concentrated ownership.
Public Investment Corporation (PIC) Governance Rating Matrix (Malan 2010:Online)	Categories related to, *inter alia*, board, individual directors, remuneration, shareholder treatment, auditing and accounting, corporate behaviour, responsibility and corporate culture based on King II recommendations.	Top 40 JSE-listed firms	N/A; Employed by the PIC for investment decision-making purposes.
South African CG disclosure index (Ntim *et al* 2012)	Index 1: four categories based on the King II Report namely: boards, directors and ownership, accounting and auditing, risk management, internal audit, and control; and compliance and enforcement. Index 2: based on disclosure relating to stakeholder practices based on the integrated sustainability reporting section of King II. Index 3: combination of the disclosure provisions of the first two indices.	169 JSE-listed firms; 2002-2007	Comprehensive disclosure of corporate governance practices pertaining to shareholders and stakeholders had a positive impact on firm value.

Source: Authors' construction

Perusal of Table 1 reveals that local researchers typically included board-related aspects, based primarily on the King II Report. Focus was placed on the disclosure of corporate governance practices by listed firms in their annual reports. The majority of the authors only examined disclosure by large listed firms and excluded small and delisted firms from their samples.

After the available instruments were evaluated, the PIC's matrix was selected, since it was regarded as the most comprehensive and well-tested local corporate governance measure. As far as could be established, this was the only instrument that included both a disclosure and an acceptability dimension. This instrument was initially designed by the Centre for Corporate Governance in Africa for the PIC, one of the largest investment managers in Africa (PIC 2015:Online). The centre agreed that this measure could be refined and applied to construct a comprehensive corporate governance database by means of content analysis.

4 RESEARCH METHODOLOGY

In this section, the selection of the sample is explained, followed by an explanation on the application of the research instrument and the data analysis techniques.

4.1 Sample selection

A combination of convenience and judgement sampling was used to draw a sample of 230 companies from six JSE industries. Based on the Industry Classification Benchmark system, companies listed in the industrials, consumer goods, consumer services, health care, technology and telecommunications industries were selected. To ensure adequate data points for statistical analysis purposes, a company had to be listed for at least two consecutive years over the period 2002 to 2010 to be included in the sample.

In line with previous researchers such as Meyer and De Wet (2013), companies listed in the basic materials, oil and gas and financials industries were excluded from the sample. The reason is the differing nature of these companies' operations and accounting conventions. In an attempt to reduce survivorship bias, listed companies and firms that delisted during the study period were incorporated in the sample. The annual reports were downloaded from the INET BFA database. Table 2 presents details on the sample companies. The number of delisted companies decreased during the study period.

Table 2: Compilation of the sample

Number of firms	2002	2003	2004	2005	2006	2007	2008	2009	2010
Listed	121	122	123	126	126	128	144	148	141
Delisted	70	70	43	35	20	13	6	3	0
Total	**191**	**192**	**166**	**161**	**146**	**141**	**150**	**151**	**141**

4.2 Application of the corporate governance research instrument

The corporate governance research instrument was refined and used to conduct a content analysis of the sample companies' annual reports. Attention was given to disclosure and acceptability criteria for nine corporate governance categories, as indicated in Table 3.

The considerable contribution of board-related categories to the total CGS is justifiable, given that the board is regarded as the focal point of the local corporate governance system (IoDSA 2002). Aspects related to corporate culture and behaviour (Category 8) made the second largest contribution to the total CGS. This high contribution is also reasonable, since there are many social considerations in the South African context, including HIV/AID and unethical behaviour such as bribery.

A list of key words was compiled for each category based on relevant literature and selected King II recommendations. These key words were used to conduct content analysis on the sample firms' annual reports. Based on their corporate governance reporting, disclosure and acceptability scores were assigned to firms. A disclosure score of 1 was allocated if information regarding a specific consideration was mentioned. An acceptability score was only assigned if the reported information conformed to the stated acceptability criteria.

A board-related example is provided to illustrate how disclosure and acceptability scores were assigned for a board composition aspect. Suppose both the chairperson of the board and the chief executive officer (CEO) were identified in a sample company's annual report. A disclosure score of 1 could be allocated, given that the role-related information was disclosed. Moreover, if the company reported that the chairperson also acted as the CEO, an acceptability score of 0 would be assigned since the King II Report recommended that the roles of these two role-players should be separated (IoDSA 2002).

The maximum CGS that could be allocated to a sample firm was 74, comprising a disclosure score of 39 and an acceptability score of 35. No acceptability criteria were set for four category-specific aspects, since the King II Report did not provide pertinent acceptability guidelines. Specific details on the individual aspects could not be disclosed due to a confidentiality agreement with the Centre for Corporate Governance in Africa. Although the King III Report came into effect on 1 March 2010, integrated reporting only became mandatory for all JSE-listed firms in 2011 (Global Sustainable Investment Alliance 2012:Online). Depending on a firm's financial year end, certain firms only started to comply with the King II Report after their 2010 financial year end. Many firms with a financial year end after 1 March 2010 aimed to comply with the King II guidelines for the largest part of their 2010 financial year. To ensure consistency, the King II recommendations were applied for the entire period.

Table 3: Structure of the refined research instrument

Corporate governance category (C)	Relevant literature	Contribution to total CGS (%)
C1: Board composition	The board is the focal point of the local corporate governance system (IoDSA 2002). Factors related to the board's composition, e.g. the status of directors, are amongst the most cited governance aspects (Abdo & Fisher 2007).	18.919
C2: Board committees	Board committees could assist board members in the performance of their duties (Mallin 2007). According to the King II Report (IoDSA 2002), a board should appoint an audit and a remuneration committee. Unless a board is very small, a nomination committee should also be established.	8.108
C3: Individual directors	Board and board committee members should devote enough time to properly fulfil their duties, such as attending meetings at various firms on which boards and board committees they serve (Harris & Shimizu 2004; IoDSA 2002).	8.108
C4: Director remuneration	Emolument packages should be sufficient to attract, retain and motivate eligible board candidates (Armstrong 2010). The King II Report (IoDSA 2002) provides detailed emolument recommendations, including that performance should be linked to remuneration.	9.459
C5: Shareholding	Listed firms should disclose their shareholder spread, pertaining to major shareholders and the percentage shares held by each (JSE 2005).	4.054
C6: Accounting and auditing	The transactions of firms should be properly accounted for. Internal auditors provide a control service and should report to the audit committee, while external auditors are expected to report an independent opinion on financial statements to stakeholders (Institute of Internal Auditors 2005:Online; IoDSA 2002).	8.108
C7: Risk disclosure and reporting	Firms are operating in an ever-changing environment, challenged by various risks. The King II Report (IoDSA 2002) suggests that directors and managers must have a thorough risk understanding and develop a risk management approach.	5.405
C8: Corporate culture and behaviour	Corporate culture refers to a pattern of shared assumptions that a company learned over time and teach to new employees (Anghel 2012). A code of ethics provides guidelines related to acceptable corporate behaviour. If firms exhibit unacceptable corporate practices, it should be addressed through litigation and the implementation of compliance functions (Heller, Murphy & Meaney 2001). Specific attention should be given to HIV/AIDS and Broad-Based Black Economic Empowerment (BBBEE) aspects (IoDSA 2002).	27.027
C9: Sustainability reporting	The King II Report recommended that attention should be given to the so-called triple bottom line performance and a firm's impact on its relevant stakeholders (IoDSA 2002). Various bodies provide sustainability-related guidelines to listed companies, including the Global Reporting Initiative.	10.811

Source: Authors' construction

4.3 Data analysis

Descriptive statistics were used to summarise the panel dataset. Specific consideration was given to compliance trends over the study period. A mixed-model repeated measures analysis of variance (ANOVA) was employed to determine whether the mean category scores differed significantly over the research period. This model, which includes fixed and random effects factors, is suitable to analyse panel data. "Year" was considered as the fixed effects factor, while "company" was regarded as the random effects factor. To estimate the variance components, a restricted maximum likelihood solution with type III decomposition was used. Since the overall F-test revealed a significant difference, the Fisher's least significant difference (LSD) test was used to make pair-wise comparisons amongst the category means to determine where the differences occurred.

5 RESEARCH FINDINGS

In this section, observed corporate governance trends are discussed. Corporate governance concerns which became evident whilst conducting content analysis will also be explained. Thereafter, the results of the mixed-model ANOVA and Fisher's LSD test are presented.

5.1 Analysing corporate governance trends

An annual CGS was composed for each of the considered firms, based on disclosure and acceptability dimensions. Table 4 provides details on the contribution of both dimensions to the average CGSs for the considered nine years.

Table 4: Mean disclosure and acceptability dimensions (% of maximum CGS of 74)

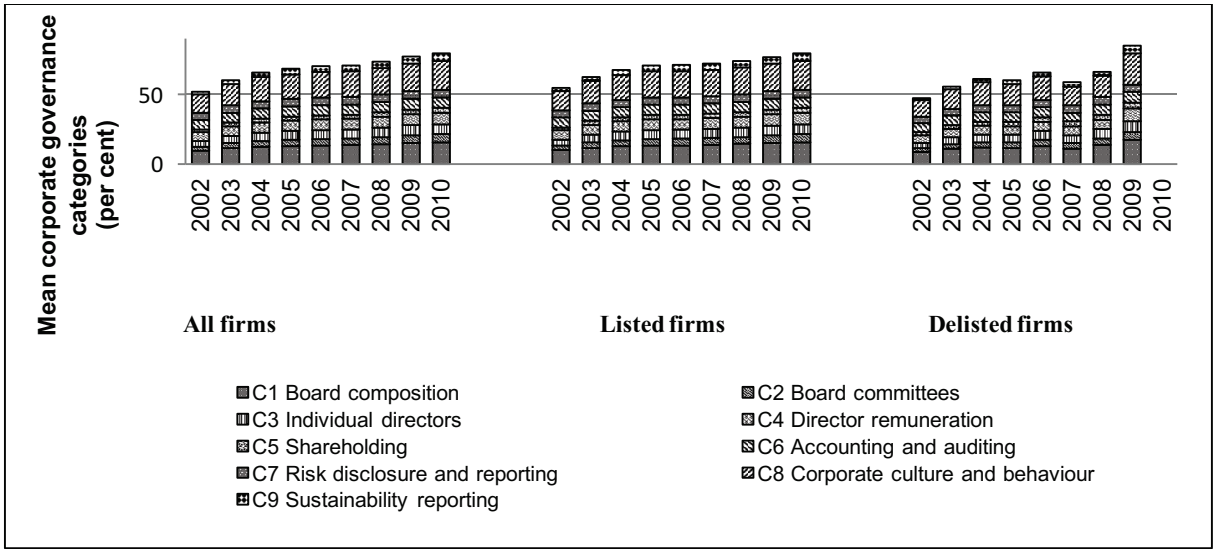
Firms	Years	2002	2003	2004	2005	2006	2007	2008	2009	2010
All	**Disclosure**	32.291	36.177	38.741	39.869	40.827	41.001	42.198	43.556	44.566
	Acceptability	19.803	24.008	27.222	28.513	29.554	29.835	31.541	33.632	34.963
	Mean CGS	52.094	60.185	65.963	68.382	70.381	70.836	73.739	77.188	79.529
Listed	**Disclosure**	33.616	37.395	39.486	40.905	41.098	41.470	42.324	43.481	44.566
	Acceptability	21.108	25.366	28.126	29.773	29.987	30.585	31.719	33.546	34.963
	Mean CGS	54.724	62.761	67.612	70.678	71.085	72.055	74.043	77.027	79.529
Delisted	**Disclosure**	30.000	34.054	36.612	36.139	39.122	36.383	39.189	47.297	n/a
	Acceptability	17.548	21.641	24.639	23.977	26.824	22.453	27.252	37.838	
	Mean CGS	47.548	55.695	61.251	60.116	65.946	58.836	66.441	85.135	

Improvements can be noted in the CSSs of the sample firms over the research period (refer to Table 4). The annual mean CGS for all the sample firms increased from approximately 52 per cent in 2002 to almost 80 per cent in 2010. Their disclosure in annual reports improved gradually over the research period. This tendency might be ascribed to the JSE Listings Requirements that obliged listed companies to disclose their compliance or explain non-compliance with the King II Report's recommendations (JSE 2005). The contribution of the acceptability dimension to the mean annual CGSs also increased over time. A possible explanation for this observation is that as time progressed, the directors of the sample firms became more accustomed with the implementation of the King II guidelines.

In 2009, three delisted firms had higher corporate governance scores than their listed counterparts. It should be noted that not all companies that delisted *per se* had poor CGSs. Some sample companies indicated that it was both costly and time-consuming to comply with the King guidelines. Compliance-related red tape might have contributed to the delisting of certain sample companies. Furthermore, sound corporate governance practices are likely to make a company an attractive target to acquire. Two of the delisted firms were involved in takeover transactions. No delisted firms were included in the sample in 2010.

The total CGSs reflected in Table 4 were based on the scores that were allocated to nine categories. The mean scores per category were converted into percentages by dividing the annual mean category scores by the maximum total CGS of 74. The category-related composition of the sample firms' annual CGSs are indicated in Figure 1. It is evident that the mean category scores for the listed firms gradually increased from 2002 to 2010. The mean category values of the delisted firms, however, fluctuated over time.

Figure 1: Mean corporate governance categories



Source: Authors' construction

As discussed, the categories did not contribute equally to the total CGS. For example, if two firms each obtained a CGS of 40 out of 74, it does not *per se* indicate that they scored equally on all categories. To determine the drivers of the improvements in the mean CGSs, the annual mean category scores for the complete sample were expressed as a percentage of the maximum total score per category. These percentages are shown in Table 5.

Table 5: Mean category scores (% of the maximum score per category)

Category (C) score	2002	2003	2004	2005	2006	2007	2008	2009	2010
C1 (out of 14)	49.550	59.786	65.964	68.857	69.964	71.479	76.193	81.029	83.436
C2 (out of 6)	38.833	46.617	51.900	54.967	59.467	59.817	62.000	66.883	71.167
C3 (out of 6)	49.133	65.017	73.500	77.017	79.800	79.900	83.450	86.750	88.183
C4 (out of 7)	69.029	71.800	76.157	78.614	79.357	80.643	83.143	86.371	87.543
C5 (out of 3)	47.633	69.267	71.300	73.700	74.667	77.067	79.100	81.667	80.367
C6 (out of 6)	85.333	86.633	87.950	90.067	90.533	90.300	91.333	94.150	95.633
C7 (out of 4)	92.800	96.350	98.200	98.125	99.325	99.300	100.000	100.000	100.000
C8 (out of 20)	48.925	56.875	64.400	65.775	68.595	67.765	70.600	73.975	75.995
C9 (out of 8)	18.188	24.225	31.250	35.563	37.675	39.100	42.250	45.200	51.688

Source: Authors' construction

The sampled companies already complied with almost 50 per cent of the stated criteria relating to the board composition (Category 1) in 2002. Considerable improvements were observed for the three board-related categories (Categories 1, 2 and 3) over time. This observation was not surprising, given

that the first King Report already discussed the role and composition of the board at length. The directors thus had more time to comply with board-specific guidelines than "more novel" considerations, such as sustainability that was introduced in the King II Report.

Reporting on director remuneration (Category 4), accounting and auditing (Category 6) and risk disclosure and reporting (Category 7) also improved over the research period. The high scores for Category 4 can be partly ascribed to the role of active shareholders and the media. These role-players often highlight remuneration-related issues, such as a lack of performance-related payment and excessive executive bonuses (De Wet 2012; Steyn 2012:Online). Revised statutory reporting requirements, such as the International Financial Reporting Standards and the JSE Listings Requirements (JSE 2005) might have steered firms towards high compliance with Category 6. All the sample firms reported on their relevant risks and the management thereof since 2008, the midst of the 2007-2009 global financial crisis.

Although below average attention was given to corporate culture and behaviour in 2002, substantial improvements were observed over time. Compliance with the sustainability reporting category was below 20 per cent in 2002. By 2010, the sample firms only complied with approximately half of the sustainability criteria. Directors and managers should hence give more attention to sustainability-related aspects, especially in light of the compulsory publishing of integrated reports since 2011. Furthermore, capital providers also give progressively more attention to environmental, social and corporate governance aspects in the aftermath of the 2007-2009 global financial crisis (United Nations Principles for Responsible Investment 2011:Online).

5.2 Category-specific observations and concerns

The authors employed content analysis as an observational research method to examine and quantify the presence and meaning of pre-defined key words in the sample firms' annual reports over almost a decade. Inferences were drawn from the messages that were conveyed to key stakeholders. The resultant category-specific observations are presented in Table 6. The authors' comments are supported by literature where applicable. Reference is also made to whether the identified aspects were addressed in the King III Report.

Table 6: Corporate governance observations based on content analysis

Category-specific observations	Supporting literature	Addressed in King III[a)]
Board composition An increase was noted in the number of NEDs over the period 2002 to 2010. A lack of independent NEDs was observed over the research period.	An independent chair can help to counter balance the influence of senior and dominant executives on the board (Gomez & Moore 2009). The likelihood of executive wrongdoing tends to decrease if the number of NEDs increases (Uzun, Szewczyk & Varma 2004).	The balance of board power was mentioned. In line with the King II Report, it was recommended that the majority of directors should be independent NEDs.
Board committees More than 50% of the sample had audit and remuneration committees by 2010. The role of the nomination committee was often combined with that of the remuneration committee. The remuneration committee's chair was often not an independent NED. Committees often comprised less than three members.	The remuneration committee assists the board to give shareholders confidence in the remuneration process and the outcomes thereof (Australian Institute of Company Directors 2004). The audit committee is regarded as essential, given that its members should review the functioning of the internal audit as well as regulatory and legal compliance functions. The committee hence has an important overseeing role (Naidoo 2002).	Reference is made to the composition of, inter alia, nomination, audit, and remuneration committees. In line with the King II Report, the majority of the committees' members should be independent NEDs.
Individual directors It seemed to be common practice for directors to serve on a number of boards. This tendency might result in over-boardedness. During the first four years of the research period, committee meeting attendance was often not disclosed for individual members. A lack of board gender diversity was noted for the majority of companies.	Over-boarded directors are those who serve on various boards simultaneously, resulting in meeting schedule conflict and the inability to efficiently conduct board duties. If the attention of a director is distracted between different firms, his/her overseeing ability decreases (Harris & Shimizu 2004). Despite advantages such as enhanced strategic decision-making, the boards of JSE-listed firms are still largely homogenous (Mans-Kemp & Viviers 2015).	Directors should not hold more directorships than what is reasonable to exercise due care. No guideline was, however, provided on the number of director-ships that might be held by a director. Although diversity was mentioned, no pertinent race and gender guidelines were given.
Director remuneration Shareholders' approval of NEDs' remuneration was often not mentioned. Furthermore, share options were given to NEDs without shareholder approval. Remuneration-related disclosure improved considerably over time. During 2008-2010, more than 50% of the sample firms provided compressive details on their directors' remuneration. In some instances, emolument benchmarks were given.	NEDs are supposed to bring independent judgement to the board. When they are rewarded with share options, unhealthy emphasis could be placed on short-term performance (Mallin 2007). Directors are likely to benefit from several excessive emolument packages if they serve on various boards (Dalton & Daily 2001).	NEDs should not receive share options or incentives linked to the share price or corporate performance. The remuneration policy should be submitted to a non-binding advisory shareholder vote at the annual general meeting. Detailed guidance was provided on NED fees and the compilation of executive remuneration.

Category-specific observations	Supporting literature	Addressed in King III[a)]
Shareholding The disclosure of shareholding information varied considerably between firms, from a detailed analysis to merely mentioning the five largest shareholders.	As the ownership structure of JSE firms became less concentrated since 1994, the number of minority shareholders increased (Habbard 2010:Online). Historically, local shareholders were passive and often did not exercise their voting rights. Shareholder activism is, however, gradually increasing, specifically pertaining to opposing executive remuneration (Viviers 2015).	Despite recognising that minority shareholders should be protected against abuse by the controlling shareholder, shareholder activism was not pertinently encouraged.
Accounting and auditing Clear indication of communication/ oversight between the internal auditor and the audit committee was often not evident in the sample firms' annual reports.	Companies that have a competent internal audit department and an efficient direct reporting line for the internal auditor often have fewer reporting problems compared to those without such a function (Albrecht, Stice, Stice & Swain 2011).	Consistent with King II, the oversight role of internal compliance officers/functions was emphasised.
Risk disclosure and reporting From 2008, all firms reported on risk management, with varying degrees of detail.	The way in which corporate role players respond to risks could mean the difference between success and failure. Risks should be managed proactively (Nolan 2007).	In line with the King II Report, a detailed discussion was provided on risk management.
Corporate culture and behaviour Most sample firms had a code of ethics which stipulated acceptable practices. More than 50% of the companies clearly mentioned their relationships with and responsibilities to their various stakeholders. A small number of firms (fewer than 10) did not mention the term stakeholder in their annual reports. Reporting on BBBEE and HIV/AIDS-related aspects improved over time.	Corporate culture tends to manifest itself in firm-specific behaviour (Anghel 2012). A firm can lose expert knowledge that was accumulated over years when a skilled employee dies of HIV/AIDS. Corporate role players should hence react sufficiently to the disease and its consequences by investing in, inter alia, internal HIV and AIDS treatment and prevention programs (Robertson 2011:Online).	The HIV/AIDS disease was not mentioned. Reference was made that a firm might fail to effectively integrate efforts related to meeting industry and government BBBEE-related requirements into its sustainability framework.
Sustainability reporting Initially, sustainability aspects were only mentioned by a few firms (approximately 20% of the sample). The number of firms that reported comprehensively on sustainability gradually increased over time.	The publication of sustainability reports by the Top 100 South African firms is gradually increasing (KPMG 2008:Online).	Listed firms should publish integrated reports, reflecting on their sustainability and financial performance.

[a)] *IoDSA (2009)*

Source: Authors' construction based on content analysis

Three main corporate governance concerns became evident whilst conducting content analysis, namely: director over-boardedness, high compliance costs and a 'tick-box' disclosure mentality. The researchers observed that certain board members served on several boards simultaneously. As a result, they might become over-boarded. This phenomenon could be partly ascribed to the limited pool of qualified and experienced black and female board candidates (Muller-Kahle, Wang & Wu 2014).

Certain sampled firms attributed their insufficient corporate governance practices to the associated costs measured in terms of time and money allocated to such practices and the proper disclosure thereof. High corporate governance costs might become disproportional to the incremental benefits, especially for small firms (Rezaee 2007). During the period 2005-2010, non-compliance with specific King II guidelines was disclosed by some firms, without providing suggestions on how such practices will be improved within the following year(s). Consequently, they adhered to the King II 'comply or explain' reporting principle (i.e. disclosed information), but they did not necessarily plan to improve their actual practices.

Some of the sampled firms' role-players seemed to have adopted a 'tick-box' approach. If directors attempt to merely comply with the basic King guidelines and hence 'tick some of the disclosure boxes', the benefits ('nuances') of effective compliance might not be obtained. Furthermore, their 'tick-box obsession' might destroy scope for flexibility pertaining to the practical application of the King guidelines (Lipton 2013:Online). An example is a CEO who also serves as the chairperson of the firm where he/she is employed. The individual might deliver outstanding service, despite the fact that his/her role-duality does not conform to the King II guideline. Some shareholders, directors and managers have publicly questioned whether 'tick-box compliance' with the King guidelines is truly an efficient measure of sound corporate governance practices (Heath 2014:Online).

According to Stürmer (2013:Online), the directors and managers of many JSE-listed firms only talk about sound corporate governance without truly practicing it. Although the mean CGSs improved over time, some sample firms exhibited a serious lack of acceptable corporate governance practices by 2010. The researchers tend to agree with Stürmer's (2013:Online) observation that certain local firms should give more attention to their inefficient corporate governance practices in order to survive and prosper over the long-term.

5.3 Mixed-model ANOVA and Fisher's LSD test results

The descriptive statistics revealed increasing trends in the mean corporate governance categories over the research period. A mixed-model ANOVA (refer to

Table 7) was employed to determine the significance of the observed trends.

Table 7: Results of the mixed-model ANOVA (mean corporate governance categories)

Fixed-effect test per corporate governance category [(a)]	F-value	p-value
Board composition	**111.391****	0.00
Board committees	**73.701****	0.00
Individual directors	**101.755****	0.00
Director remuneration	**17.504****	0.00
Shareholding	**46.691****	0.00
Accounting and auditing	**11.450****	0.00
Risk disclosure and reporting	**4.676****	0.00
Corporate culture and behaviour	**86.252****	0.00
Sustainability reporting	**71.661****	0.00

*** Significant at the 1% level * Significant at the 5% level*
[(a)] Fixed-effect: year; Random effect: company
Numerator degrees of freedom 8; Denominator degrees of freedom 1 197
Source: Authors' analysis

As seen in Table 7, all the mean category scores differed significantly over the research period. It could be expected that the corporate governance practices and reporting of JSE-listed firms would improve, as their directors, managers and accountants became more familiar with the King guidelines over time. JSE-listed firms were required to disclose their compliance or explain non-compliance with the King II recommendations (JSE 2005). It is, however, possible that some sample firms did not improve the acceptability of their practices *per se*, but merely developed their disclosure and non-compliance explanations over time.

Some of the sample firms that improved their corporate governance disclosure over the duration of the research period stated that it takes time to create efficient corporate governance and reporting mechanisms. A Fisher's LSD test (Table 8) was conducted for three periods, namely: 2002 and 2004; 2005 and 2007 and 2008 and 2010 to determine whether the differences in the mean category scores were significant.

Table 8: Results of the Fisher's LSD test

Corporate governance categories	2002 and 2004		2005 and 2007		2008 and 2010	
	Mean difference	P-value	Mean difference	P-value	Mean difference	P-value
C1: Board composition	**2.144****	0.00	0.295	0.07	**0.951****	0.00
C2: Board committees	**0.738****	0.00	**0.270****	0.00	**0.533****	0.00
C3: Individual directors	**1.405****	0.00	0.107	0.24	**0.244****	0.01
C4: Director remuneration	**0.342****	0.00	0.097	0.31	**0.243***	0.01
C5: Shareholding	**0.713****	0.00	0.099	0.14	0.076	0.27
C6: Accounting and auditing	0.090	0.11	0.033	0.58	**0.226****	0.00
C7: Risk disclosure and reporting	**0.150****	0.00	-0.006	0.87	0.006	0.88
C8: Corporate culture and behaviour	**2.822****	0.00	0.274	0.20	**0.869****	0.00
C9: Sustainability reporting	**0.984****	0.00	**0.234***	0.05	**0.723****	0.00

*** Significant at the 1% level * Significant at the 5% level*
Source: Authors' analysis

Perusal of Table 8 reveals considerable improvements for all categories over the first part of the study period (2002-2004), except for accounting and auditing. The average score for this category only increased by approximately 3 per cent during this period. Figure 1 revealed small categorical improvements over the following three years. The insignificant Fisher's LSD test results for most categories between 2005 and 2007 were not unexpected.

Significant improvements were observed for most categories between 2008 and 2010. The categories that revealed insignificant results respectively improved with approximately 1 per cent (shareholding) and zero per cent (risk disclosure and reporting). Corporate governance mechanisms were criticised for failing to safeguard listed firms against excessive risk-taking prior to the 2007-2009 global financial crisis (Erkens, Hung & Matos 2012). Since 2008, the mid-point of this crisis period, more emphasis was placed on the acceptability of corporate governance practices. Such pressure might have encouraged the sample companies to improve their actual corporate governance practices and the disclosure thereof for the last part of the study period.

6 CONCLUSIONS, LIMITATIONS AND RECOMMENDATIONS

South Africa is regarded as a corporate governance pioneer, not only in Africa, but globally. The King Reports have provided corporate governance guidance to listed firms since 1994. Few authors, however, comprehensively assessed the corporate governance practices of JSE-listed firms. This research was presented from a King II perspective. In line with previous researchers, the authors evaluated the disclosure of corporate governance in 1 439 annual reports of listed companies. The sample included 230 firms over the period 2002 to 2010. Attention was also

given to the acceptability of the disclosed information (i.e. whether it conformed to specific King II guidelines), hence contributing to the current body of knowledge.

Improvements were noted in the average disclosure and acceptability scores over the research period. Significant improvements were also observed for most categories for the periods 2002 and 2004, and 2008 and 2010. Specific caveats, however, became evident whilst conducting content analysis. It seemed as if the correct application of the King II guidelines and the philosophy behind the report was not properly understood by all role-players by 2010.

Directors probably require more training on their roles, responsibilities and ethical decision-making. In addition, if a director acts contrary to a firm's ethical values, his/her contract should not be renewed or be terminated if the case warrants it. It is recommended that directors should limit their board memberships to give sufficient attention to the activities of all firms which they serve.

Although information on the corporate governance achievements of certain firms were reported in the media and on their websites, such information was not always properly disclosed in their annual reports. It hence seems as if accountants also require enhanced training to assist firms to appropriately report their financial and sustainability-related performance, especially given the advent of integrated reporting. The media can expand their role from merely exposing unacceptable practices to reporting corporate governance success stories, thereby encouraging debate on acceptable practices.

A limitation of the study is that companies that were listed in the oil and gas, basic materials and financials industries were excluded from the sample. The reason was the differing nature of the activities, the degree of regulation and the financial reporting of firms operating in these industries in comparison to the sampled firms. The sample was consequently not representative of all JSE-listed firms, but only of the considered industries.

A suggestion for future research is to examine the corporate governance compliance practices as reported in the integrated reports of mining and financial companies since 2011. Interviews could also be conducted with board members to discuss possible reasons and solutions to address the problem of over-boardedness.

Acknowledgements

This article forms part of a more comprehensive PhD study. The authors would like to thank the Centre for Corporate Governance in Africa at the University of Stellenbosch Business School for the permission to use a refined version of their PIC Corporate Governance Rating Matrix. The authors also extend their gratitude to Professor Martin Kidd for his assistance with the statistical analysis and the National Research Foundation for financial support.

REFERENCES

Abdo, A. & Fisher, G. 2007. The impact of reported corporate governance disclosure on the financial performance of companies listed on the JSE. *Investment Analysts Journal*, 36(66):43-56.

Albrecht, W.S., Stice, E.K., Stice, J.D. & Swain, M.R. 2011. *Accounting concepts and applications*. 11th edition. Mason, OH: South-Western Cengage Learning.

Anghel, G. 2012. *Doomed to internationalization and modernization of corporate culture: The Russian experience of German firms*. Wiesbaden: Gabler Verlag.

Armstrong, M. 2010. *Armstrong's handbook of reward management practice: Improving performance through reward*. 3rd edition. London: Kogan Page.

Australian Institute of Company Directors. 2004. *Remuneration committees: Good practice guide*. Sydney: Australian Institute of Company Directors.

Boubaker, S. & Nguyen, D.K. 2014. *Corporate governance in emerging markets: theories, practices and cases*. New York: Springer.

Carte, D. 2009. King 3's too soft. *Moneyweb*, 19 May. [Online]. http://www. moneyweb.co.za/moneyweb-corporate-governance/king-3s-too-soft (Accessed: 10 June 2014).

Corporate Governance Framework Research Institute. 2016. *Corporate governance quotes*. [Online]. http://www.corporate-governance.co.za/Home/CorporateGovernanceQuotes/tabid/148/Default.aspx (Accessed: 21 September 2016).

Dalton, D.R. & Daily, C.M. 2001. Director stock compensation: An invitation to a conspicuous conflict of interests? *Business Ethics Quarterly*, 11(1):89-108.

De Wet, J.H.V.H. 2012. Executive compensation and the EVA and MVA performance of South African listed companies. *Southern African Business Review*, 16(3):57-80.

Eccles, N.S., De Jongh, D., Nicholls, S.J., Sinclair, G. & Walker, P. 2007. The state of responsible investment in South Africa. [Online]. http://www.unepfi.org/fileadmin/documents/The_State_of_Responsible_Investment_01.pdf (Accessed: 2 October 2015).

Erkens, D.H., Hung, M. & Matos, P. 2012. Corporate governance in the 2007-2008 financial crisis: Evidence from financial institutions worldwide. *Journal of Corporate Finance*, 18(2):389-411.

European Corporate Governance Institute (ECGI). 2013. *Index of all codes*. [Online]. http://www.ecgi.org/codes/all_codes.php (Accessed: 1 July 2013).

European Corporate Governance Institute (ECGI). 2015. *Index of all codes*. [Online]. http://www.ecgi.org/codes/all_codes.php (Accessed: 12 May 2015).

Freeman, R.E. 1984. *Strategic management: A stakeholder approach*. Boston: Pitman.

Global Sustainable Investment Alliance. 2012. *Global sustainable investment review*. [Online]. http://gsiareview2012.gsi-alliance.org/index.html#/1/. (Accessed: 24 February 2015).

Gomez, P-Y. & Moore, R. 2009. *Board members and management consultants: Refining the boundaries of consulting and corporate governance*. New York: Information Age.

Habbard, P. 2010. Corporate Governance in South Africa. *Hans-Böckler-Foundation research paper. Trade Union Advisory Committee to the Organisation for Economic Co-operation and Development*. [Online]. http://www.tuac.org/en/public/e-docs/00/00/08/60/ document_doc.phtml (Accessed: 19 September 2016).

Harris, I.C. & Shimizu, K. 2004. Too busy to serve? An examination of the influence of over boarded directors. *Journal of Management Studies*, 41(5):775-798.

Heath, A. 2014. The chatter: top talent can wear two hats in era of many rules. *Business Day Live*, 10 August. [Online]. http://www.bdlive.co.za/businesstimes/2014/08/10/ the-chatter-top-talent-can-wear-two-hats-in-era-of-many-rules (Accessed: 10 August 2014).

Heller, J.C., Murphy, J.E. & Meaney, M.E. 2001. *Guide to professional development in compliance*. Gaithersburg: Aspen.

Institute of Directors in Southern Africa (IoDSA). 1994. *King Report on Corporate Governance*. Johannesburg: IoDSA.

Institute of Directors in Southern Africa (IoDSA). 2002. *King Report on Corporate Governance for South Africa-2002*. Johannesburg: IoDSA.

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

Institute of Internal Auditors. 2005. *Audit committee briefing … internal audit standards: Why they matter*. [Online]. http://www.theiia.org/download.cfm?file= 83632 (Accessed: 12 May 2015).

Johannesburg Stock Exchange (JSE). 2005. *JSE Listings Requirements*. Durban: LexisNexis Butterworths.

John, K. & Makhija, A.K. 2011. *International corporate governance*. Bingley: Emerald Group Publishing.

Jones, T.M. & Felps, W. 2013. Stakeholder happiness enhancement: a neo-utilitarian objective for the modern corporation. *Business Ethics Quarterly*, 23(3):349-379.

KPMG. 2008. *KPMG international survey of corporate responsibility reporting 2008*. [Online]. http://www.kpmg.com/GR/en//IssuesAndInsights/articlesPublications/Sustainability/Documents/Surveyof CorporateResponsibilityReporting2008.pdf (Accessed: 7 May 2011).

Lipton, M. 2013. *The Bebchuk syllogism*. [Online]. http://blogs.law.harvard.edu /corpgov/2013/08/26/the-bebchuk-syllogism/ (Accessed: 10 February 2015).

Malan, D. 2010. *Rating corporate governance: the delicate balance between disclosure, compliance and performance*. [Online]. http://www.slideserve.com/denzel/unit-for-corporate-governance-in-africa (Accessed: 14 May 2015).

Malherbe, S. & Segal, N. 2001. *Corporate governance in South Africa*. Paper presented at the Trade and Industrial Policy Strategies 2001 Annual Forum, 10-12 September, Muldersdrift, South Africa.

Mallin, C.A. 2007. *Corporate governance*. 2nd edition. Oxford: Oxford University Press.

Mangena, M. & Chamisa, E. 2008. Corporate governance and incidences of listing suspension by the JSE Securities Exchange of South Africa: An empirical analysis. *The International Journal of Accounting*, 43(1):28-44.

Mans-Kemp, N. & Viviers, S. 2015. Investigating board diversity in South Africa. *Journal of Economic and Financial Sciences*, 8(2):392-414.

Meyer, E. & De Wet, J.H.V.H. 2013. The impact of board structure on the financial performance of listed South African companies. *Corporate Board: Role, Duties and Composition*, 9(3):29-41.

Moloi, S.T.M. 2008. *Assessment of corporate governance reporting in the annual reports of South African listed companies*. Unpublished Master of Commerce thesis, University of South Africa, Pretoria, South Africa.

Muller-Kahle, M.I., Wang, L. & Wu, J. 2014. Board structure: An empirical study of firms in Anglo-American governance environments. *Managerial Finance*, 40(7):681-699.

Naidoo, R. 2002. *Corporate governance: An essential guide for South African companies*. Cape Town: Juta.

Nolan, J. 2007. *Corporate accountability and triple bottom line reporting: Determining the material issues for disclosure*. [Online]. http://papers.ssrn.com/sol3/papers.cfm?abstract_ id=975414 (Accessed: 23 March 2015).

Northrup, C.L. 2006. *Profitable Sarbanes-Oxley compliance: attain improved shareholder value and bottom-line results*. Boca Raton: Ross Publishing.

Ntim, C.G., Opong, K.K. & Danbolt, J. 2012. The relative value relevance of shareholder versus stakeholder corporate governance disclosure policy reforms in South Africa. *Corporate Governance: An International Review*, 20(1):84-105.

Organisation for Economic Co-operation and Development. 2007. *Recent trends and regulatory implications in socially responsible investment for pension funds*. [Online]. http://www.oecd.org/dataoecd/3/0/38550550.pdf (Accessed: 21 November 2014).

Pretorius, L. 2011. Growing African roots. *Financial Mail*, 18 August. [Online]. http://www.fm.co.za/ Article.aspx?id=151080 (Accessed: 25 January 2012).

Public Investment Corporation (PIC). 2015. *Welcome to the Public Investment Corporation*. [Online]. http://www.pic.gov.za/ (Accessed: 8 May 2015).

Rezaee, Z. 2007. *Corporate governance post-Sarbanes-Oxley regulations, requirements and integrated processes*. Hoboken: Wiley.

Robertson, M. 2011. *HIV/AIDS: An issue for responsible investors?* [Online]. http://www. eiris.org/blog/hivaids-an-issue-for-responsible-investors/ (Accessed: 21 February 2012).

Steyn, L. 2012. Keeping tabs on executive pay. *Mail and Guardian*, 24 May. [Online]. http://mg.co.za/article/2012-05-24-keeping-tabs-on-executive-pay (Accessed: 3 June 2015).

Stürmer, A. 2013. Governance risks high for SA. *Management SA*, 15 July. [Online]. http://managementsa.co.za/ governance-risks-high-for-sa/ (Accessed: 13 May 2014).

United Nations Principles for Responsible Investment. 2011. *Responsible investment in private equity*. [Online]. http://www.unpri.org/wp-content/uploads/PE_Guide_2.pdf (Accessed: 10 June 2015).

Uzun, H., Szewczyk, S.H. & Varma, R. 2004. Board composition and corporate fraud. *Financial Analysts Journal*, 60(3):33-43.

Van den Berghe, L. & De Ridder, L. 1999. *International standardisation of good corporate governance: Best practices for the board of directors*. Boston: Kluwer Academic Publishers.

Viviers, S. 2015. Executive remuneration in South Africa: Key issues Highlighted by shareholder activists. *African Journal of Business Ethics*, 9(1):1-28.

Weimer, J. & Pape, J.C. 1999. A taxonomy of systems of corporate governance. *Corporate Governance: An International Review*, 7(2):152-166.

Disclosure of independence-enhancing attributes within the audit committee/ internal audit activity relationship

K Barac
Department of Auditing
University of Pretoria

JT Mdzikwa
Department of Auditing
University of Pretoria

ABSTRACT

Independence is a cornerstone of the internal audit profession, hence its prominence in the definition of internal auditing. The quality of the audit committee/internal audit activity relationship is important for the enhancement of the independence of the internal audit activity. Using content analysis, this article examines attributes within the audit committee/internal audit activity relationship. Information disclosed in the annual reports of the Top 40 companies listed on the Johannesburg Stock Exchange on the internal audit activity was used during the content analysis. The findings revealed that most companies did not disclose the selected attributes extensively in their annual reports. Since there are no legislative requirements on the extent to which such disclosures should appear in the annual reports of companies in respect of the internal audit activity, the results of this study can be used by the internal audit standard setters to advance their work in this area.

Key words

Annual report disclosure; internal audit activity; Top 40 JSE listed companies; audit committee; internal auditor independence

1 INTRODUCTION

Von Eck (2013:Online), the chief executive officer (CEO) of the Institute of Internal Auditors South Africa (IIA SA), posted an article on the IIA SA's blog page entitled "Have we created a generation of bullies?" In the article, she indicates that she has listened to numerous internal auditors recounting incidents of intimidation and victimization by senior individuals within their organizations. She even went as far as to reveal that in certain instances intimidation and victimization were of such a magnitude that the lives and/or posts of internal auditors were specifically threatened (Von Eck 2013Online). Internal auditors are in a unique position that allows them insight into their organizations, including their most sensitive matters (Soh & Martinov-Bennie 2011:605). Thus, the occurrence of wrongdoing, such as fraud and corruption, within an organization, could first be detected and reported by internal auditors (Ahmad 2011:25; Barac & Coetzee 2012:33). This situation (being the discoverer of a significant act of wrongdoing) could be a contributing factor to internal auditors being intimidated and victimized, and which, if allowed to continue, could threaten their independence and compromise their authority and effectiveness.

The independence of the internal audit activity (IAA) is sufficiently important to be a specific component of the definition of internal audit. Independence is defined as "the freedom from conditions that threaten the ability of the IAA to carry out internal audit responsibilities in an unbiased manner" (IIA 2012). When an IAA is not independent, its authority may be weakened and thus rendering it vulnerable to challenges by management, and its contribution may be disregarded (Mahzan, Zulkifli & Umor 2012:71). Together with the IIA's professional standards (Standards) (IIA 2012) and the *King Code of Governance for South Africa* (King III Report) (IoD, 2009), the literature recognizes various attributes of the function that confirm that when present, the authority of the IAA is established and its independence is strengthened. These attributes include: the IAA's reporting lines; the need for an approved internal audit charter; the need for the formal approval of the internal audit plan, and audit committee (AC) approval of the hiring or dismissal of the chief audit executive (CAE) (Christopher, Sarens & Leung 2009:204; Mahzan *et al* 2012:69-71). The IAA should report functionally to the AC (Soh & Martinov-Bennie 2011:615) and the AC is required to approve the IAA's charter (Sarens & De Beelde 2006:225; IIA, 2012). These reporting lines and attributes serve as indicators of the quality of the relationship between the AC and the IAA. Stewart and Subramaniam (2010:333) posit that "A quality relationship between the IAA and the AC also works towards providing the IAA with the appropriate

environment and support system for carrying out its own governance related activities". Thus, the AC plays a vital role in enhancing the independence of the IAA (Goodwin & Yeo 2001:107; Christopher *et al* 2009: 215; Marx & Voogt 2010:20).

An AC is a sub-committee of the board of directors (IoD 2009). A well-composed AC is an important corporate governance structure, which is also tasked with overseeing the IAA (Goodwin 2003:263; IoD 2009:63; Schneider 2010:19). The IAA is influential as it can enhance the effectiveness of the AC by updating the AC on developments in legislation, and educating the AC members on their (changing) roles and responsibilities, amongst other issues (Moorthy, Seetharaman & Saravanan 2010:91; Lin, Pizzini, Vargus & Bardhan 2011:290; Mahzan *et al* 2012:72). A quality relationship between the AC and the IAA is thus critical to enhancing the independence of the IAA (Christopher *et al* 2009:15). Previous research has illustrated the importance of this AC/IAA relationship describing it in various ways. This is confirmed by the publication of comments such as: the AC/IAA relationship is one of mutual dependence and symbiosis; the IAA is the "eyes and ears" or "legs and arms" of the AC; the IAA is the watchdog of the AC; the IAA is the comfort provider to the AC; and the AC is viewed as a key safeguard mechanism for the IAA (Marx & Voogt 2010:18; Stewart & Subramaniam 2010:333; Lenz & Sarens 2012:538; Azza 2012:iii).

A broad body of knowledge exists on how the AC should support the IAA and thus enhance its independence. Numerous research studies have identified and highlighted attributes that contribute to developing a quality relationship between the AC and the IAA, thereby enhancing the independence of the IAA. Such attributes include the following: the AC approves the IAA's resources, internal audit plan, internal audit charter, and staffing complement; the AC supports the IAA having private meetings with the CAE; the AC also follows up on matters reported to it by the IAA; and it arbitrates on matters of disagreement arising between the IAA, management and external auditors (Goodwin & Yeo 2001:110; Alleyne, Howard & Greenidge 2006:569; Ferreira 2007:9; Van der Nest, Thornhill & De Jager 2008:552; Stewart & Subramaniam 2010:334; IIA 2012; Mahzan *et al* 2012:77).

The CAE drives the internal audit quality and is a link between the IAA, the AC and management (Coetzee, Fourie, Plant & Barac 2013:56). The success of the IAA is thus dependent on the good standing of the CAE, which is in turn founded on the CAE being in possession of a postgraduate academic qualification, professional certification, and a minimum of ten years of internal auditing experience (Coetzee *et al* 2013:57). Furthermore, the CAE should have management and leadership skills, communication skills, independence and objectivity, and an ability to partner with management and the AC (Mahzan *et al* 2012:93; Coetzee *et al* 2013:56), in the interests of the organisation. If the CAE commands these personal attributes, such an individual is less likely to be coerced into performing actions that might compromise the independence of the IAA. Nevertheless, to strengthen the IAA's independence, the AC should play a role in the appointment and dismissal of a CAE; review the performance of the CAE and advise the remunerations committee regarding the remuneration of the CAE. If these actions are undertaken by the AC, the IAA's staff is less likely to feel that their job security is dependent on management's good opinions of their jobs, and their independence should be enhanced (Goodwin & Yeo 2001:110; Goodwin 2003:271; Christopher *et al* 2009:204; IoD 2009:63; Marx & Voogt 2010: 22; IIA 2012:4).

From the above it is clear that various attributes within the AC/IAA relationship have the potential to influence the independence of the IAA. The disclosure of the presence and status of these attributes in the annual report would, therefore, enable users of the financial statements to evaluate the degree of independence enjoyed by the IAA. Since the IAA is regarded as a governance mechanism and type of internal control, if it is perceived to be independent, investors may then perceive the organization's control environment to be sound, and that the organisation is safe (sufficiently low risk) for investment (Moorthy *et al* 2010:91-96; UNCTAD 2010:20). It is against this backdrop that this study analyses the disclosure of the IAAs' independence-enhancing attributes in the AC/IAA relationships of the Top 40 JSE-listed companies (as presented in their annual reports), to determine the degree to which the information that influences the independence of the IAA is formally disclosed. A number of studies have been conducted on the independence of the IAA; however, these studies have been conducted with the objective of understanding the relationship between the AC and the IAA (Goodwin & Yeo 2001:107; Goodwin 2003:263; Christopher *et al* 2009:200). Although these studies highlight the role of the AC in enhancing the independence of the IAA, they do not investigate whether these specific attributes within the AC/IAA relationship that would enhance the independence of the IAA, are publicly disclosed. The study reported on in this article aims to close this gap.

The remainder of the article conforms to the following structure: the following section presents the problem statement, and the objective, scope, limitations and significance of the study. Thereafter, a review of published literature is reported on, the methodology and design of the research is described, and the findings of the study are presented. In the final section, the conclusions reached are presented, and recommendations are made.

2 PROBLEM STATEMENT

There are no legislative requirements to guide the AC on what disclosures should be made regarding the presence or absence of independence-enhancing attributes within the AC/IAA relationship, which probably explains why this matter has received so little attention from researchers. This could be seen as a shortcoming in business-specific legislation, since the IAA is now regarded as an important corporate governance mechanism (Holt 2012:881). Holt (2012:881) explains that although there are

mandatory corporate disclosure requirements about the AC, management and external auditors, there are no mandatory disclosures about the IAA. Therefore, he suggests that companies voluntarily disclose the composition, responsibilities and activities of their IAAs to enhance the credibility of their other disclosures and financial results (Holt 2012:881).

Marx and Voogt (2010:24) conducted a study to determine the extent to which the ACs' reports on their oversight of the IAA addressed key independence-related issues. They investigated the ACs' involvement in the appointment or dismissal of the CAE; the sign-off of the internal audit plan; responses to findings arising from the internal audit; co-operation between the internal and external audit functions, and the degree to which internal audit had access to the chairperson of the AC and the board. The findings of their study revealed that even though the AC has an increasing number of functions and responsibilities to fulfil in respect of the IAA, its disclosures in the annual report remain limited in number and depth (Marx & Voogt 2010). In a more recent study, Chambers and Odar (2015:41) noted that although the IAA has a direct reporting relationship with the board and the AC, the low number of related disclosures reported remains a concern. This could be due to the sensitive nature of some of the issues discovered, the disclosure of which could reflect badly on those charged with governance. Furthermore, as noted by Chamber and Odar (2015:45), the IAA is not empowered to make unilateral public disclosures if the board has not sanctioned the release of such information. In order to address this issue, the IAA is formulating a mandatory guidance note regarding when such unauthorized public disclosure by internal audit would be appropriate (Chambers & Odar 2015:46). Against this background, a study of the disclosures relating to the independence of the IAA is not only timeous but also relevant.

3 OBJECTIVES, SCOPE, LIMITATIONS AND SIGNIFICANCE OF THE STUDY

The objective of this study is to analyze those independence-enhancing attributes of the IAA within the AC/IAA relationship that have been disclosed in the annual reports of the Top 40 JSE-listed companies published between 2012 and 2013. Information on ACs and IAAs disclosed in these annual reports was analyzed and interpreted to shed light on the AC/IAA relationship as described in the literature review. However, a limitation of the study is that the analysis of the disclosures of attributes that enhance the independence of the IAA within the AC/IAA relationship was limited to scrutiny of those published in the annual reports of the Top 40 JSE-listed companies. Although restricting the research to the review of the annual reports may be seen as a limitation, the annual report is an important company document and a key channel for communication with stakeholders: it provides the reader with her first impression of the company's compliance with corporate governance requirements, as well as its wider sense of accountability (UNCTAD 2006:29; Barac & Moloi 2010:20).

The thematic analysis approach, as part of the content analysis research method used to evaluate the annual reports, has inherent limitations. It risks conveying an incomplete picture of the company's business as it focuses on words and numbers, and may, by ignoring the graphics and pictures that are not always fully described in supporting paragraphs, give an incomplete view of the message the company is attempting to communicate (Barac & Moloi 2010:20). Furthermore, content analysis does not have an intrinsic theoretical base, and thus inferences may be drawn too liberally, and relationships and impacts implied in a study may be disregarded, thereby drawing inaccurate inferences (Bryman, Bell, Hirschsohn, Dos Santos, Du Toit, Masenge, Van Aardt & Wagner 2014:299-305; CSU [n.d]:27; Mouton 2001:166). Another risk integral to content analysis is its ability to re-code data the same way over an extended period of time, without considering how information and practices change over that period, which opens the research to accusations of inaccurate information and conclusions (CSU 2004:27).

These above-mentioned limitations are applicable to this study, since the documents analyzed are the annual reports of the Top 40 JSE-listed companies for FY2012/3. However, the limitations are countered through conscious adoption of a syncretic view of the contents of the various sections of each annual report (usually structured as an overview, corporate governance review and the financial statement sections). This was intended help to establish links between various styles of presentation of information (annual reports are usually the products of a team of authors) and to enhance the accuracy of the conclusions. In addition, the thematic analysis is set out in Table 1 to facilitate comparable follow-up studies (Bryman *et al* 2014:299-305). Despite these limitations, content analysis remains an acceptable method of coding annual reports as it can extract information that is not otherwise prominently quantified (Leedy & Ormond 2005:145).

Management of organizations and their AC members should recognize the benefits arising from applying the findings of the study because the disclosure of the IAA's independence-enhancing attributes within the AC/IAA relationship sends a strong signal to stakeholders that the AC has fulfilled its oversight duty. Stakeholders may then use the disclosed attributes as a yardstick to determine the degree of independence enjoyed by the IAA, and thus of the organization's corporate governance performance. Since investors enjoy peace of mind when investing in organizations with demonstrably sound corporate governance, the disclosure of the attributes should demonstrate the AC's commitment to transparency and to enhancing the IAA's independence. Furthermore, the users of the financial statements could benefit from an enhanced focus on internal audit disclosures, and the IIA could use the findings of the study as inputs to improve disclosure requirements with respect to the IAA.

4 LITERATURE REVIEW

4.1 Why organizations need an internal audit activity

Corporate scandals such as Enron and WorldCom brought significant public and regulatory attention to corporate governance (Goodwin & Yeo 2001:108; Savcuk 2007:275; Archambeault, De Zoort & Holt 2008:376). Furthermore, the demand for internal assurance on the effectiveness of corporate governance, internal controls and risk management increased (Goodwin & Yeo 2001:108; Savcuk 2007:275; Archambeault *et al* 2008:376). Since the IAA is uniquely positioned to provide such internal assurance, public expectations of the function's efforts grew rapidly. The heightened interest in IAAs resulted in the recognition that a proactive IAA was needed, which in turn powered the demand for improvements in internal audit quality. Simultaneously, the need for the visibility and relevance of the IAA to be improved, and for their skills to be put to effective use was recognized. This was a radical change from the then norm where the IAA's presence was for little more than "tick-box" compliance purposes (Marx & Voogt 2010:17; Moorthy *et al* 2010:90; Mutai 2011:7; Soh & Martinov-Bennie 2011:606; Lenz & Sarens 2012:534).

Over the subsequent 10 - 15 years, the role of internal auditing has evolved to the point that it is now a key corporate governance mechanism, providing independent assurance on the effectiveness of the company's governance processes, and includes prevention of wastage through fraud, corruption, unethical behaviour and "irregularities" (Mihret, James & Mula 2010:225; Stewart & Subramaniam 2010:4; Soh & Martinov-Bennie 2011:606). The need for internal auditing has been driven by guidance in the King III Report that recommends all companies should have effective IAAs. In the event that a company decides not to establish an IAA, full reasons justifying this decision should be disclosed in its integrated report, together with an explanation of how adequate assurance of an effective governance, risk management and internal control environment has been maintained (IoD 2009:93). The UK Corporate Governance Code, in contrast to the King III code, does not specifically require companies to establish and maintain an IAA; however, it does require that in cases where there is no IAA, ACs should annually consider whether there is perhaps a need for an IAA, and if so, make recommendations to the board (FRC 2012:19). In addition, the reasons for the (continuing) absence of such a function are required to be explained in the relevant sections of the annual report (FRC 2012:20).

The increase in business complexity presents the IAA with an opportunity to help the organization to achieve its business objectives (Savcuk 2007:275). Because the IAA is independent and objective, its review of the organization's state of economy, efficiency and effectiveness enables the AC to make informed decisions about the status of the organization's internal corporate governance, risk management, internal control and compliance functions and efforts (Mihret *et al* 2010:225; Soh & Martinov-Bennie 2011:606). However, in that the AC requires an objective assurance, independent of management, and the IAA is in a position to offer such assurance (Chambers 2014:197), it is vital that this independence and objectivity is demonstrably protected and promoted. Furthermore, external auditors have also come to trust and use the IAA's knowledge of the business, and rely on its independence and experience (Suwaidan & Qasim 2010:509). In addition, the IAA is well-positioned to assist and advise the board and management. Thus, their input is sought on how to apply corporate governance principles, and how to execute business strategy. They are also asked to make recommendations to address weaknesses in internal controls, counter unethical behavior and to respond to regulatory changes. In addition, they are sometimes asked to make informed decisions in respect of acquisitions and mergers, and on how to protect the assets, reputation and sustainability of the organization (Moorthy *et al* 2010:91; Soh & Martinov-Bennie 2011:611; Lin *et al* 2011:287; Mahzan *et al* 2012:70-74; Chambers 2014:199).

4.2 Why should the internal audit activity be independent?

The above discussion highlights the need for an IAA. However, the value the IAA adds to the organization may be diluted or disregarded if it is not independent of management and other extraneous influences (Stewart & Subramaniam 2010:320). The concept of internal auditor independence is widely championed by academic research and endorsed by business practice (Sarens & De Beelde 2006:220; Stewart & Subramaniam 2010:327; Schneider 2010:19). It is in the core of the definition of internal auditing, being described as "an independent, objective assurance and consulting activity" (Stewart & Subramaniam 2010:330; Schneider 2010:19; Leung, Cooper & Perera 2011:794; IIA 2012). It is embedded in the International Standards for the Professional Practice of Internal Auditing (generally referred to as the Standards) which requires internal auditors to be independent both in fact and appearance (IIA 2012); in addition, they should be "seen" and be "heard" to be independent (Al-Ajmi & Saudagaran 2011:131). Other best practices, such as those contained in King III Report, recommend that companies have an effective IAA that is independent, objective and strategically positioned, so that it is able to contribute effectively to corporate governance (IoD 2009:97).

According to the source credibility theory, individuals place more reliance on information provided by an IAA, than they do on other sources because they perceive the IAA to be credible and reliable (Holt 2012:884). Thus, the AC, which does not have direct access to the same level of information as management (since it is not involved in the day-to-day operations of the organization), relies on the IAA to obtain and present it with the credible and reliable information it requires in order to make informed decisions, and to exercise oversight in the best interests of the organization (Marx & Voogt 2010:22; Mutai 2011:18; Soh & Martinov-Bennie 2011:615).

The credibility and reliability of the information obtained is directly linked to the degree of independence the IAA enjoys (Holt 2012:884). In addition, an independent IAA commands company-wide respect and can be perceived by the stakeholders as aiding senior executives fulfil their desire to achieve business objectives (Stewart & Subramaniam 2010:329; Holt 2012:884). Other stakeholders who benefit from the independence of the IAA are the external auditors. Ebaid (2011:114) states that to decide on whether or not to place reliance on the work of the IAA (whether or not to view IAA as reliable and credible), external auditors consider a number of variables, including the IAA's independence and objectivity.

The IAA plays a prominent role in the organization's internal control structures, and is seen as an internal control component itself (Mihret *et al* 2010:240; Yasin & Nelson 2012:188). Over and above the fact that the IAA is an internal control, it also examines and evaluates the adequacy and effectiveness of other controls and this is where its independence and objectivity become critical (Marx & Voogt 2010). An IAA that lacks independence and/or objectivity is likely to be influenced by management, which weakens its effectiveness as an internal control. This lack of independence can constitute a material weakness, compromising the entire system of internal control, thereby increasing the likelihood of misstatements in the annual and interim financial statements (Hermanson, Ivancevich & Ivancevich [n.d]:21; Lin *et al* 2011:293). The view held by certain executives and managers (that internal auditors are their employees, and that their reporting to the AC is little more than a formality to satisfy corporate governance requirements), places the IAA open to manipulative abuse by management, thereby weakening its independence (Van Peursem 2005: 490; Sarens & De Beelde 2006:223; Christopher *et al* 2009:203; Schneider 2010:19).

4.3 Independence-enhancing attributes within the AC/IAA relationship and the importance of their disclosure

It is recommended that for good corporate governance to be effected, the IAA should report functionally to the AC and administratively to the chief executive officer (IoD 2009:96; Stewart & Subramaniam 2010:333). As previously discussed, the independence of the IAA is strengthened when it reports to a level in the organization that permits it to fulfill its responsibilities free from interference or influence (IIA 2012; Holt 2012:880). From an administrative reporting perspective, such a level is one held by an executive with sufficient authority to promote the independence of the IAA; from the functional reporting perspective, such a level is that of the AC (Stewart & Subramaniam 2010:331; IIA 2012). Holt (2012:883) highlights that functional reporting involves the governance-related activities of the IAA, such as charter approval, hiring or terminating the CAE and receiving periodic results of IAA's investigations. Administrative reporting involves the day-to-day activities of the IAA, including human resource administration, budgeting, and the administration of internal policies and procedures.

According to the IIA (2012), there are actions (attributes) that specifically establish functional reporting. These actions are: the approval of the IAA's charter by the AC and the board; approval of the risk-based internal audit plan by the AC and the board; and the CAE communicates the IAA's performance relative to its plan, and other matters, directly to the AC and the board. In addition, the AC and the board approve the remuneration of the CAE, the IAA's resources, and decisions regarding the appointment or removal of the CAE. Finally, the AC and the board make appropriate enquiries of management and the CAE to determine whether the audit's scope and the allocated resources are sufficient for the intended purposes. In view of the fact that functional reporting to the AC enhances the IAA's perceived independence (Stewart & Subramaniam 2010:331; IIA 2012), these actions/attributes can be regarded as enhancing the independence of the IAA, albeit still within the AC/IAA relationship. These aforementioned functional reporting actions/attributes are also included in the model audit charter the IIA has developed for the IAA (IIA 2013) and which is also used in legislated governance and professional regulations (FRC 2003:12; IoD 2009; IIA 2013).

A number of studies have analyzed the actions required to establish functional reporting lines for the IAA, and have related them to the strength of the AC/IAA relationship. Among these studies is that of Savcuk (2007:278), who analyzed the independence of an IAA in Greece by examining the AC/IAA relationship, looking for evidence of the AC's approval of the appointment or dismissal of the CAE, the AC's approval of the IAA's resources and audit plans, and for the IAA's reports and recommendations. In a study in South Africa, Barac, Plant and Motubatse (2009:982-986) also reported on these functional reporting-specific attributes/actions implicit in a quality AC/IAA relationship, and found them to be in place. A study conducted by Goodwin and Yeo (2001:110) presents corroborating findings. The Joint Inspection Unit (JIU) conducted a review of the efforts of the IAA in the United Nations system organizations, with a view to improving system-wide coherence among entities dealing with the IAA (JIU 2010:7). To enhance the effectiveness and efficiency of the IAA in the United Nations system organizations, the JIU identified attributes prerequisite for an independent IAA; these are closely aligned with the functional reporting-specific attributes discussed above and viewed as essential to enhancing the quality of the AC/IAA relationship.

Established, functional reporting lines seem to enhance the effectiveness of the AC/IAA relationship over time. This relationship is important since it should provide the IAA with an appropriate environment and support system from which to execute its governance activities (Stewart & Subramaniam 2010:333; Marx & Voogt 2010:18; Lenz & Sarens 2012:538). Since functional reporting establishes the working relationship between the AC and the IAA, it can be inferred that the previously discussed functional reporting-specific attributes enhance the AC/IAA relationship, thus strengthening the independence of the IAA (IoD 2009:93; Soh

& Martinov-Bennie 2011:615; IIA 2012). The functional reporting-specific attributes, regarded as independence-enhancing attributes, comprise the basis for the fieldwork in this study.

Since this study focuses on the AC/IAA relationship, a brief discussion of the AC is now essential. The AC is a subcommittee of the board of directors, tasked with overseeing the IAA (Schneider 2010:25; Soh & Martinov-Bennie 2011:615; Lary & Taylor 2012:336). Arising from the aftermath of the many corporate collapses in the early 2000s, regulatory authorities in many national jurisdictions made the establishment of ACs compulsory for companies (Schneider 2010:25; Soh & Martinov-Bennie 2011:615). However, these companies soon became aware that the mere existence of ACs would not necessarily reduce the frequency or extent of corporate collapses; a significant requirement was, therefore, introduced to legislation, regulations and guidelines, being that in order for ACs' operations to be effective the ACs should be independent of influence from boards of directors and management (Baxter 2010:57; Magrane & Malthus 2010:427; Kang, Kilgore & Wright 2011: 623). The AC's effectiveness is thus strengthened by enhancing its key characteristics; particularly its independence, expertise, size and its activity level (Baxter 2010:58). An effective AC thereby enhances the independence of the IAA, amongst other benefits (IoD 2009:69).

Certain legislative efforts such as *Sarbanes-Oxley Act* in the USA, and best practice such as King III Report in South Africa, require ACs to disclose (usually in the AFS) the status of the internal controls (IoD 2009; Haron, Ibrahim, Jeyaraman & Chye 2010:142; Ali 2014:133). Earlier it was noted that Mihret *et al* (2010:230) and Yasin and Nelson (2012:188) have viewed the IAA as an internal control. By virtue of an IAA now being recognized as an internal control, the AC has to disclose the status of the IAA. Holt (2012:881), as well as Soh and Martinov-Bennie (2011:607), believe that although there are as yet no mandated disclosures about the status of a company's IAA, this should not prevent the disclosure of such information. The AC's report seems to be a useful vehicle for such disclosures. They further maintain that since the effectiveness of the IAA (which includes the IAA's independence) enhances the credibility of the information reported, such a disclosure on the status of the IAA will be in the best interest of the company (Holt 2012:881; Soh & Martinov-Bennie 2011:607). Haron *et al* (2010:142) support this view, indicating that voluntary disclosures (i.e. disclosures over and above the minimum disclosures required by law or regulation), send a positive signal to stakeholders about management's commitment to internal controls, and their commitment to the protection of company assets and shareholders' investments.

Haron *et al* (2010:156 & 157) discuss items that could be disclosed voluntarily in respect of the IAA. They suggest that the IAA's direct reporting relationship to the AC, the approval of the IAA's charter by the AC, the AC's approval of the hiring or dismissal of the CAE, as well as CAE's remuneration should be disclosed voluntarily. Such a call for the voluntary disclosure of independence-enhancing attributes within the AC/IAA relationship is an indication that their disclosure is important. Holt (2012:881) notes that investors do value disclosures on independence-enhancing attributes relating to AC/IAA relationship, since such disclosures enhance the investors' confidence on the effectiveness of the AC's oversight efforts. When investors are confident about the effectiveness of the AC's oversight of the IAA, they can comfortably form an opinion about the effectiveness of the organization's control environment, as well as the reputation of the IAA. This opinion could impact their investment decision-making processes (Moorthy *et al* 2010:91-96; UNCTAD 2010:20). Other important benefits following disclosure of independence-enhancing attributes within the AC/IAA relationship include: enhancing shareholder confidence in the organization's management, and the reliability and credibility of financial reporting; demonstrating the organization's compliance with laws and regulations and management's commitment to transparency and good corporate governance, and enhancing external stakeholders' confidence regarding the organization's oversight effectiveness (Archambeault *et al* 2008:376; Lary & Taylor 2012:336). Of great importance is the fact that such disclosure also helps external stakeholders to evaluate the independence of the IAA and thus to form an opinion about the role it plays in governance (Archambeault *et al* 2008:379-382).

5 METHODOLOGY AND RESEARCH DESIGN

The study uses the empirical method known as content analysis to examine the independence-enhancing attributes of the IAA within the AC/IAA relationship. A thematic analysis (a part of content analysis), was used, requiring the researcher to code text in terms of themes (Bryman *et al* 2014). Content analysis is a systematic, rigorous research approach used to analyze passages within documents obtained or generated in the course of research (Bryman *et al* 2014:299-305; CSU [n.d]:1). This method is also referred to as document analysis, which is defined by Bowen (2009:28) as a systematic procedure for reviewing or evaluating documents, both printed and electronic. Content analysis requires a detailed and systematic examination of the contents of a particular body of material in order to identify patterns and themes (Leedy & Ormrod 2005:142). Furthermore, its claim to research rigor rests in its ability to make replicable and valid inferences from texts (CSU [n.d]:2); U.S GAO 1989:8).

Although content analysis has been used to complement other research methods, it has also been utilized as a stand-alone method, particularly in specialized qualitative research studies (Bowen 2009:29). Bowen's endorsement of content analysis as a stand-alone method is supported by Stewart and Subramaniam (2010:333), who used the method in a study in which only the AC charters and reports of 150 US companies were examined, in preference to the more time-consuming alternative of conducting surveys and face-to-face interviews. Furthermore, Dumay and Cai (2015:131) assert that content

analysis is also appropriate where direct observational evidence is not available. The use of content analysis in the aforementioned studies supports and strengthens the authors' choice of content analysis as a stand-alone research method appropriate for this current study.

The study was conducted by identifying themes that enable the analysis of IAAs' independence-enhancing attributes within their AC/IAA relationships, using disclosures in the annual reports of the Top 40 JSE-listed companies. The JSE's Top 40 Index (based on market capitalization), as quoted by I-Net Bridge on September 2014, was used to identify the companies for this study (I-Net Bridge 2014:Online). The 2012/13 annual reports of the selected companies were downloaded from the companies' websites, and the sections containing the corporate governance reports (particularly the ACs' reports on their IAAs) were analyzed. Annual reports were used for the analysis because these reports are considered to be the primary mediums for communicating with the public. In addition, annual reports also contain other useful information, enable the companies to connect with their internal and external stakeholders, and be used collectively as a barometer of the attitudes of companies towards reporting (Guthrie, Petty, Yongvanich, & Recceri 2004:287; Dumay & Cai 2015:125). The 2012/13 financial year was chosen, as it was the most recent complete source of published data available to the authors (this study commenced during the 2014 financial year). In addition, since this study did not seek to establish trends in disclosures of independence-enhancing attributes of IAAs over a period of years, the focus on a single financial year was appropriate and sufficient. Bowen (2009:28) posits that even though researchers review prior literature with the intention of incorporating it in their current work, all the analyzed documents are not necessarily considered for the current study, as they may not have been found to be relevant. Thus, following Bowen's notion, the analysis of the prior years' annual reports was seen as unnecessary as it did not help the authors to achieve the objective of the study (essentially, to benchmark the state of the relationship as it existed at the end of the 2012/3 financial year).

The annual report is a publication comprising financial and non-financial reports. Included amongst the non-financial reports is the corporate governance report. Although the AC/IAA relationship-enhancing attributes are reported in the corporate governance section of the non-financial report, the annual report was analyzed in its entirety, seeking to corroborate the information, to give it wider context and to make sense of it.

A further justification for the use of content analysis for this study is that it is less time-consuming, and more efficient in comparison to other research methods. In addition, most documents are in the public domain; the method is less costly to conduct than interviews and surveys, and the documents are not affected by the research process. These documents can be repeatedly reviewed, and conclusions can be drawn based on the content evidence, without having to access unwilling and inaccessible communicators. As an effective research method, it has been used for many decades to study performance and reporting, as it creates a picture of a given phenomenon, as opposed to describing reality objectively (Beattie & Thomson 2006:3; White & Marsh 2006:38; Bowen 2009:31; Kusuma 2013:9; Moolman, Cronje & Wingard 2001:5; Barac & Moloi 2010:19; Bhasin 2012:59).

Although content analysis is a widely acknowledged research method, it has inherent limitations. As used in this study, the following potential limitations are recognized. The information reported by the AC is prepared for general reporting purposes and not necessarily to satisfy (or even be aware of) the needs of academic research. Additionally, the information reported on the IAA's independence-enhancing attributes may be specific to a particular company's unique policies and business environment. Thus, the analysis, findings and conclusions may not be generalizable across the business universe. Information on the IAA's independence-enhancing attributes may be inaccurate, short on quantity/depth or excessively detailed, and there may be an element of subjectivity in both content and layout that could affect how the information is assimilated and coded by the researchers (Guthrie *et al* 2004:289; Bowen 2009:29; Goebel 2015:683; Dumay & Cai 2015:125).

Thematic analysis as part of content analysis: implementation steps

Step 1: Review the literature pertaining to the IAA's independence with respect to its relationship with ACs and identify and understand currently recognized attributes of the relationship that enhance the independence of the IAA.

Step 2: Identify data and select a sample. FY 2012/2013 annual governance reports of the Top 40 JSE-listed companies were accessed from the companies' websites. The data (the text of the governance reports within the annual reports) was extracted.

Step 3: Determine the content unit; select the unit of analysis from reports. The content unit is the portion/extent of written material that is to be examined for categories of words or statements. The unit can be a chapter, section, paragraph or a sentence in length, depending on the type of content being analyzed (Zhang & Wildemuth [n.d]:5; U.S GAO 1989:1; Cooper & Schindler 2001:430). Report sections with headings "audit committee" and "internal audit" were selected as content units.

Step 4: Identify themes or categories (outlined in Table 1): These form the heart of content analysis. They provide the structure for grouping recording units and are generated by grouping observations that are similar or related (Prasad [n.d]:11; Zhang & Wildemuth [n.d]:3-5; U.S GAO 1989:11).

Step 5: Develop the recording units (also outlined in Table 1): These are "specific segments of the context unit in the written material that is placed in a category", which can be a word, a group of words, a

sentence, a paragraph or an entire document (U.S GAO 1989:10). The recording units were developed from reviewing the annual report analysis, with particular focus on the ACs' reports on the IAAs.

Step 6: Develop and apply the codes for the themes or categories: Coding entails assigning an identifier (key word) to a theme or category and subsequently to a recording unit within that theme or category. This is equated to developing a dictionary and can be done using a computer or manually. For the purpose of this study, manual coding was used by using the keywords listed in Table 1.

Step 7: Analysis and interpretation of results: Coded data was analyzed, leading to the identification of patterns within the recording units of the sampled companies.

Step 8: Validity: Establish whether the results of this study were consistent with other studies (they were) (Barac & Moloi 2010; Holt 2012; Marx & Voogt 2010).

Step 9: Reliability: Determine whether the recording units identified during the analysis of the annual reports were supported by literature (they were).

Table 1: Summary of categories, codes and recording units

Themes or categories	Recording units	Key words
1. AC support for the IAA	1.1 Approval of the IAA budget	Budget
	1.2 Confirmation of the IAA resources	Resources, sources
	1.3 Approval of the IAA plan	Plan, planning
	1.4 CAE's access to the board	Board access
	1.5 CAE's access to the AC chairperson	AC access, chairperson
	1.6 Private meetings with the AC chairperson	Private meetings
2. Authority of the IAA	2.1 Approval of the IAA charter	IAA charter
	2.2 Administrative reporting to chief executive officer	Administrative, reporting
	2.3 Functional reporting to AC	Functional, reporting
3. Employment of the CAE	3.1 Appointment of the CAE supported by the AC	Appointment, CAE
	3.2 Dismissal of the CA supported by audit committee	Dismissal, CAE
	3.3 Performance evaluation of the IAA (relative to plans)	Performance evaluation
	3.4 Determination of CAE's remuneration	Remuneration, CAE

6 PRESENTATION OF FINDINGS

Figure 1 presents the results of the analysis of the attributes that enhance the IAA's independence within the AC/IAA relationship, as disclosed in the annual reports of the Top 40 JSE-listed companies. The results highlight the existence of an unsatisfactory position of their disclosure, which reveals areas for improvement. The contextualization of "fully disclosed", "partly disclosed" and "not disclosed" is explained in Appendix A.

The analyzed results revealed that of the 13 identified attributes, only one was reported on in the majority of the companies' annual reports. Twenty three (57.5%) of the companies sampled fully disclosed that the AC had approved the IAA's plan. Nineteen (47.5%) of the companies fully disclosed information on the IAA charter. Such disclosures arguably demonstrate that the primary focus of ACs is on the IAA's plan and charter. This observation is closely aligned to findings published by Marx and Voogt (2010), who found that 100% of ACs reviewed the IAA's plan and charter.

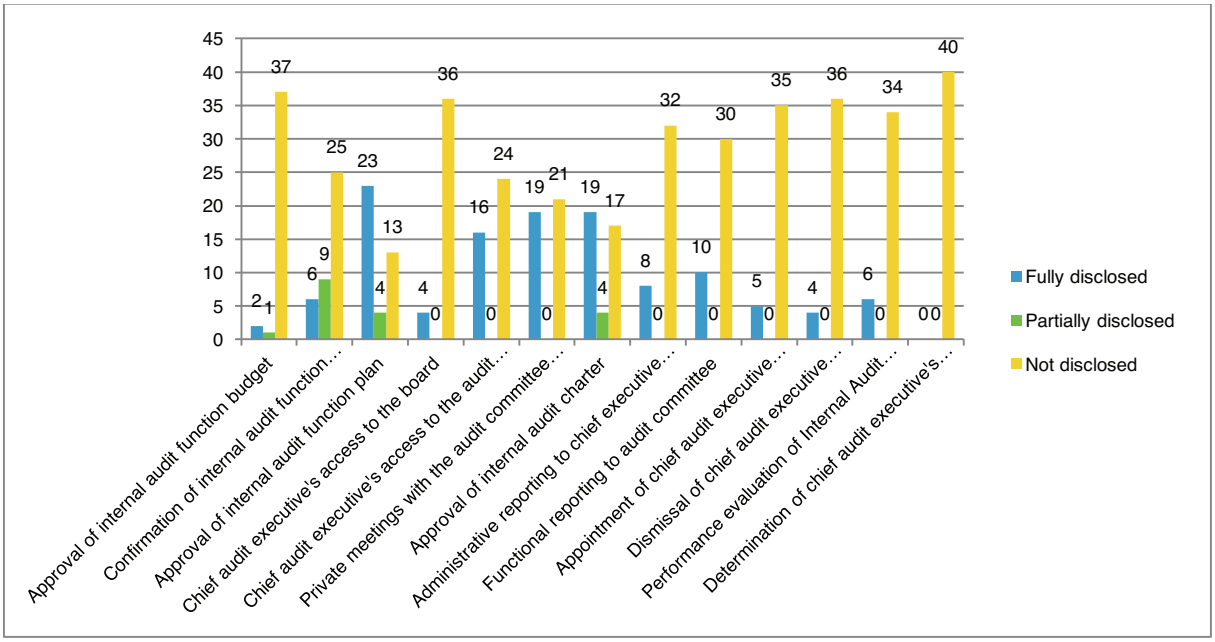
Another attribute that received some prominence is that of the CAE's access to the AC: 16 (40%) of the selected companies fully disclosed this information. However, none of them disclosed whether the CAE's remuneration had been approved by the AC. This finding is closely aligned with those in the study conducted by Ernst & Young in 2006, in which it was found that only 8% of ACs had approved the remuneration of CAEs (Marx & Voogte 2010).
Most of the Top 40 JSE-listed companies in this present study did not disclose the bulk of the attributes identified as capable of enhancing the IAA's independence within the AC/IAA relationship. Attributes which are generally omitted include: the approval of IAA budget; confirmation of the IAA's resources; confirmation of the CAE's access to the board; confirmation of the CAE's access to the AC; confirmation of administrative reporting to the CEO; confirmation that the appointment of the CAE was supported by AC; dismissal of CAE supported by AC, and the evaluation of the IAA's performance relative to approved plans.

This research finding revealed that there is a relatively low level of disclosure on the presence or otherwise of independence-enhancing attributes within the AC/IAA relationship and this is consistent with that of Marx and Voogt (2010:24). They found that although the AC fulfills various functions and responsibilities in respect of the IAA, disclosures of these in the annual reports remain limited. The finding is also aligned to that of Holt (2012:879) who found that external stakeholders have no information about the composition, responsibilities or activities of the IAA. The most cost-effective way of communicating this information to external stakeholders should be in the companies' annual reports. Furthermore, this agrees with the finding by Barac and Moloi (2010:23) in their study entitled "An assessment of corporate governance reporting in the annual reports of South African listed companies", where they observed that there was at best only partial disclosure of information in respect of internal audit independence.

Overall, the findings of this study provide evidence of a minimalist approach to disclosure regarding the presence of independence-enhancing attributes within the AC/IAA relationship in South Africa's Top 40 JSE-listed companies. Furthermore, the findings

give an updated perspective on the state of the disclosure of these independence-enhancing attributes within the AC/IAA relationship in the Top 40 JSE listed companies, and this contributes to the body of literature on the subject. In addition, these findings have implications for the internal audit profession's standard setters, as they highlight, among others, a probable need to compel the disclosure of the state of compliance with IAA independence-enhancing attributes, so as to address the impact of their non-disclosure. Furthermore, the findings question the need and importance to fully disclose these attributes and this could inform future regulation and direct future research.

Figure 1: Analysis of the independence-enhancing attributes within AC/IAA relationship as disclosed in the annual reports of the Top 40 JSE listed companies



7 CONCLUSIONS AND RECOMMENDATIONS

The existence of an IAA increases the likelihood that a company will detect and report fraud themselves: thus, its establishment is in the best interest of the company. The company derives value from an independent IAA as it is then able to resist pressure from management, and conducts audits in accordance with the professional standards of the internal audit profession. A good (well-defined and managed) AC/IAA relationship is important for the enhancement of the independence of the IAA. Previous research, in addition to regulations and guidelines, have identified and alluded to various attributes within the AC/IAA relationship that enhance the independence of the IAA.

The objective of this study was to use thematic analysis (as part of content analysis) to analyze the annual reports of the Top 40 JSE-listed companies to determine if there has been disclosure of such independence-enhancing attributes within the relationship between their ACs and IAAs. The results revealed that companies do not disclose these attributes extensively in their annual reports. This lack of extensive disclosure raises questions, as demonstrable independence is the cornerstone supporting the continuing existence of the internal audit profession; information revealing the ongoing independence of the IAA could, therefore, be of significant value to users of financial statements, as well as to internal auditors desiring to retain their relevance on the payroll.

A lack of disclosure of independence-enhancing attributes with respect to the IAA could create an impression that the AC lacks commitment to ensuring the organization's internal controls remain effective, and to establishing an optimal working relationship with the IAA. Report recommends that ACs should provide a "description of [their] working relationship" with the CAE (IoD, 2009:69). As an area for future research, the investigation as to whether users of financial statements need (or even consider) information on the independence of the IAA, and if so, to identify their preferred disclosures, would be instructive. As the amendment to King III Report is currently being debated, the achievement of clarity on what the "description of the working relationship" should entail, and of the supporting legislative requirements to guide disclosures regarding the independence of the IAA could be most useful.

Since the IAA's independence-enhancing attributes within the AC/IAA relationship considered in this study relate specifically to the establishment of the functional reporting of the IAA, the lack of extensive disclosure raises doubts about the existence of effective functional reporting *per se*, and thus of the very independence of the IAA] The lack of extensive disclosure on the status of the IAA's independence-enhancing attributes could create an impression that the AC does not see value in confirming the independence of the IAA, and it thus lacks commitment to internal controls. This might well influence stakeholders, both by inhibiting their ability to evaluate the effectiveness of the IAA, and to be

assured of their independence. This then obviously represents an area ripe for future research, particularly in light of recent studies that have questioned the value proposition of internal auditors (Lenz & Hahn 2015). A future study could, therefore, determine whether this could be addressed by the ACs disclosing the presence of independence-enhancing attributes within the IAA.

This article focused on analyzing the AC/IAA relationship as disclosed in the annual reports of the Top 40 JSE-listed companies to determine the presence of attributes that enhance the independence of the IAA. Future research could expand this understanding by analyzing the annual reports of government institutions, and particularly state-owned entities to identify whether (and if so, the degree to which) these entities report on the attributes that enhance the independence of their IAAs. Another area that may be useful to explore is the determination of the extent of IAA independence when reporting through modes of communication other than companies' annual reports.

REFERENCES

Ahmad, S.A. 2011. Internal auditors and internal whistleblowing intentions: A study of organizational, individual, situational and demographic factors. *Unpublished master's thesis*, Edith Cowan University, Western Australia.

Al-Ajmi, J. & Saudagaran, S. 2011. Perceptions of auditors and financial statement users regarding auditor independence in Bahrain. *Managerial Auditing Journal*, 26(2):130-160.

Ali, A.A.R. 2014. Corporate governance: The role and effectiveness of the audit committee in Bahrain. *International journal of business and management*, 9(3):131-137.

Alleyne, P., Howard, M. & Greenidge, D. 2006. The role of audit committees in Barbados. *Corporate Governance*, 6(5):567-581.

Archambeault, D.S., De Zoort, F.T. & Holt, T.P. 2008. The need for an internal audit report to external stakeholders to improve governance transparency. *Accounting Horizons*, 22(4):375-388.

Azza, W.A. 2012. Perceived effectiveness of the internal audit function in Libya: A qualitative study using institutional and Marxist theories. *Unpublished master's thesis*. University of Southern Queensland, Australia.

Barac, K. & Coetzee, G.P. 2012. The effect of specific internal audit function features on the demand for internal auditors in South Africa. *Southern African Journal of Accountability and Auditing Research*, 13:33-45.

Barac, K. & Moloi, T. 2010. Assessment of corporate governance reporting in the annual reports of South African listed companies. *Southern African Journal of Accountability and Auditing Research*, 10:19-31.

Barac, K., Plant, K. & Motubatse, K.N. 2009. Perceptions on the value added by South African internal audit functions. *African Journal of Business Management*, 3(13):980-988.

Baxter, P. 2010. Factors associated with the quality of audit committees. *Pacific accounting review*, 22(1):57-74.

Beattie, V. & Thomson, S.J. 2006. Lifting the lid on the use of content analysis to investigate the intellectual capital disclosures. Discussion paper series in the Accountancy and Finance, School of Management and Languages. [Online]. http://www.sml.hw.ac.uk/.../dp2006-af01.pdf (Accessed: 15 November 2014).

Bhasin, M. 2012. Audit committee scenario and trends in a developing country. Bang College of Business, KIMEP University. [Online]. http://www.iiuedu.eu/press/.../BME_Article7.pdf (Accessed: 15 November 2014).

Bowen, G.A. 2009. Document analysis as a qualitative research method. *Qualitative research journal*, 9(2):27-40.

Bryman, E., Bell, P., Hirschsohn, A., Dos Santos, J., Du Toit, A., Masenge, I., Van Aardt, & C. Wagner. 2014. Research methodology. *Business and management contexts* (pp. 213-241). Cape Town: Oxford University Press.

Chambers, A.D. 2014. Commentary: new guidance on internal audit: an analysis and appraisal of recent developments. *Managerial Auditing Journal*, 29(2):196-218.

Chambers, A.D. & Odar, M. 2015. A new vision for internal audit. *Managerial Auditing Journal*, 30(1):34-55

Christopher, J., Sarens, G. & Leung, P. 2009. A critical analysis of the independence of the internal audit function: evidence from Australia. *Accounting, Auditing and Accountability Journal*, 22(2):200-220.

Coetzee, G.P., Fourie, H., Plant, K. & Barac, K. 2013. Internal audit competencies: skills requirements for chief audit executives in South Africa. *Southern African Journal of Accountability and Auditing Research*, 15:53-63.

Colorado State University (CSU). [n.d]. Content analysis. [Online]. http://writing.colostate.edu/guides/guide.cfm?guideid=61 (Accessed: 20 September 2014).

Colorado State University (CSU). 2004. An introduction to content analysis. [Online]. http://writing.colostate.edu/references/research/content/com2d2.cfm (Accessed: 20 October 2014).

Cooper, D.R. & Schindler, P.S. 2001. *Business research methods*. New York: McGraw-Hill, 12th edition.

Dumay, J. & Cai, L. 2015. Using content analysis as a research methodology for investigating intellectual capital disclosure; a critique. *Journal of intellectual capital*, 16(1):121-155.

Ebaid, I.E. 2011. Internal audit function: An exploratory study from Egyptian listed firms. *International journal of law and management*, 53(2):108-128.

Ferreira, I. 2007. The role of internal auditors in the professional development of audit committee members. *Unpublished master's thesis*, University of South Africa, Pretoria, Gauteng Province, South Africa.

Financial Reporting Council (FRC). 2003. Audit committees: Combined code of guidance. [Online]. <http://www.frc.org.uk/.../guidanceonAuditCommittees> [Accessed: 13 October 2014].

Financial Reporting Council (FRC). 2012. The UK corporate governance code. [Online]. http://www.frc.org.uk/.../Corporate Governance (Accessed: 11 October 2014).

Goebel, V. 2015. Is the literature on content analysis of intellectual capital reporting heading towards a dead end? *Journal of intellectual capital*, 16(3):681-699.

Goodwin, J. 2003. The relationship between the audit committee and the internal audit function: Evidence from Australia and New Zealand. *International Journal of Auditing*, 7:263-278.

Goodwin, J. & Yeo, T.Y. 2001. Two factors affecting internal audit independence and objectivity: Evidence from Singapore. *International Journal of Auditing*, 5:107-125.

Guthrie, J., Petty, R., Yongvanich, K. & Recceri, F. 2004. Using content analysis as a research method to inquire into intellectual capital reporting. *Journal of intellectual capital*, 5(2):282-293.

Haron, H., Ibrahim, D.D.N., Jeyaraman, K. & Chye, O.H. 2010. Determinants of internal control characteristics influencing voluntary and mandatory disclosures: A Malaysian perspective. *Managerial auditing journal*, 25(2):140-159.

Hermanson, D.R., Ivancevich, D.M. & Ivancevich, S.H. [n.d]. Building an effective internal audit function: Learning from SOX Section 404 reports. St. John's University. [Online]. http://www.econbiz.de/Record/building-an-effective-internal-audit-function-learning-from-sox-section-404-reports-hermanson-dana/10009911725 (Accessed: 5 October 2014).

Holt, T.P. 2012. The effects of internal audit role and reporting relationships on investor perceptions of disclosure credibility. *Managerial auditing journal*, 27(9):878-898.

Institute of Directors Southern Africa (IoD). 2009. *King report on corporate governance* for South Africa. Johannesburg: IoD.

Institute of Internal Auditors (IIA). 2012. International standards for the professional practice of internal auditing (standards). Altamonte Springs: IIA.

Institute of Internal Auditors (IIA). 2013. Model internal audit activity charter. Altamonte Springs: IIA.

I-Net Bridge. 2014. FTSE/JSE: AFR TOP 40 (Daily). [Online]. http://www.thebeststockbroking.co.za/downloads/stockselectmonthly.pdf (Accessed: 26 October 2014).

Joint Inspection Unit [JIU]. 2010. The audit function in the United Nations system. Geneva: United Nations.

Kang, W.S., Kilgore, A. & Wright, S. 2011. The effectiveness of audit committees for low- and mid- cap firms. *Managerial auditing journal*, 26(7):623-650.

Kusuma, M. 2013. Does culture tame the bunny? Content analysis of a global adult magazine. Qualitative market research: *An international journal*, 17(1):4-23

Lary, A.M. & Taylor, D. W. 2012. Governance characteristics and role effectiveness of audit committees. *Managerial Auditing Journal*, 27(4):336-354.

Leedy, P.D. & Ormrod, J.E. 2005. *Practical research: planning and design*. 9th edition. New Jersey: Pearson.

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

Lenz, R. & Hahn, U. 2015. A synthesis of empirical internal audit effectiveness literature pointing to new research opportunities. *Managerial Auditing Journal*, 30(1):5–33.

Leung, P., Cooper, B.J. & Perera, L. 2011. Accountability structures and management relationships of internal audit: An Australian study. *Managerial auditing journal*, 26(9):794-816.

Lin, S., Pizzini, M., Vargus, M. & Bardhan, I. 2011. The role of the internal audit function in the disclosure of material weaknesses. *The Accounting Review, American Accounting Association*, 86(1):287-323.

Magrane, J. & Malthus, S. 2010. Audit committee effectiveness: a public sector case study. *Managerial auditing journal*, 25(5):427-443

Mahzan, N., Zulkifli, N. & Umor, S. 2012. Role and authority: An empirical study on internal auditors in Malaysia. *Asian Journal of Business and Accounting*, 5(2):69-98.

Marx, B. & Voogt, T. 2010. Audit committee responsibilities vis-à-vis internal audit: How well do top 40FTSE/JSE-listed companies shape up? *Meditari Accountancy Research*, 18(1):17-32.

Mihret, D.G., James, K. & Mula, J.M. 2010. Antecedents and organizational performance implications of internal audit effectiveness: Some proposition and research agenda. *Pacific accounting review*, 22(3):224-252.

Moolman, S., Cronje, C.J. & Wingard, H.C. 2001. Intellectual capital: Measurement, recognition and reporting. *Unpublished master's thesis*. University of South Africa, Pretoria, Gauteng Province, South Africa.

Moorthy, M.K., Seetharaman, A. & Saravanan, A.S. 2010. The realities of auditor independence and objectivity. *Journal of Accounting, Business and Management*, 17(1):90-103.

Mouton, J. 2001. *How to succeed in your masters and doctoral studies: A South African guide and resource book*. Pretoria: Van Schaik.

Mutai, P.K. 2011. Empirical study on the effectiveness of audit committee in public sector: A case study of government ministries in Kenya. *Unpublished master's thesis*, University of Nairobi, Kenya.

Prasad, B.D. [n.d]. Content analysis: A method in social science research, New Delhi: Rawat. [Online]. http://www.css.ac.in/.../content%20analysis.%... (Accessed: 13 November 2014).

Sarens, G. & De Beelde, I. 2006. The relationship between internal audit and senior management: A qualitative analysis of expectations and perceptions. *International Journal of Auditing*, 10:219-241.

Savcuk, O. 2007. Internal audit efficiency evaluation principles. *Journal of Business Economics and Management*, VIII(4):275-284.

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

Soh, D.S.B & Martinov-Bennie, N. 2011. The internal audit function: Perceptions of internal audit roles, effectiveness and evaluation*. Managerial Auditing Journal*, 26(7):605-622.

Stewart, J. & Subramaniam, N. 2010. Internal audit independence and objectivity: emerging research opportunities. *Managerial Auditing Journal*, 25(4):328-360.

Suwaidan, M.S. & Qasim, A. 2010. External auditors' reliance on internal auditors and its impact on audit fees: An empirical investigation. *Managerial auditing journal*, 25(6):509-525

United Nations Conference on Trade and Development (UNCTAD). 2006. Guidance on good practices in corporate governance disclosures. Geneva: UNCTAD.

United Nations Conference on Trade and Development (UNCTAD). 2010. Corporate governance in the wake of the financial crises. Geneva: UNACTAD.

United States General Accounting Office (GAO). 1989. Content analysis: A methodology for structuring and analyzing written material. [Online]. http://www. Achive.gao.gov/d48t13/138426.pdf. (Accessed: 20 October 2014).

Van der Nest, D.P., Thornhill, C. & De Jager, J. 2008. Audit committees and accountability in the South African public sector. *Journal of Public Administration*, 43(4):545-558.

Van Peursem, K.A. 2005. Conversations with internal auditors, the power of ambiguity. *Managerial* Auditing Journal, 20(5):489-512.

Von Eck, C. 2013. Have we created a generation of bullies? [Online]. http://www.iiasa.org.za/blogpost/889226/169260/Have-we-created-a-generation-of-bullies (Accessed: 6 October 2014).

White, M.D. & Marsh, E.E. 2006. Content analysis: A flexible methodology. *Library trends*, 55(1):22-45.

Yasin, F.M. & Nelson, S.P. 2012. Audit committee and internal audit: Implications on audit quality. *International Journal Of Economics, Management And Accounting*, 20(2):187-218.

Zhang, Y. & Wildemuth, B.M. [n.d]. Qualitative analysis of content. [Online]. http://www.ischool.utexas.edu (Accessed: 11 July 2014).

APPENDIX A: CONTEXTUALIZATION OF THE MEANING OF FULLY, PARTLY AND NOT DISCLOSED

Recording unit	Fully disclosed	Partly disclosed	Not disclosed
1.1 Approval of IAA budget	The IAA is agreed upon by the AC	The IAA reviewed by the AC; no mention that it was agreed upon or approved	Not mentioned at all
1.2 Confirmation of the IAA resources	The AC reviewed and agreed on the sufficiency of IAA's resources	The AC reviewed the IAA's resources, but no confirmation of sufficiency	Not mentioned at all
1.3 Approval of the IAA plan	The IAA plan is reviewed and agreed upon by the AC	The IAA's plan is reviewed but not agreed upon	Not mentioned at all
1.4 CAE's access to the board	Reported that the CAE has access to the board	Not applicable	Not mentioned at all
1.5 CAE's access to the AC chairperson	Reported that CAE has access to the AC chairperson	Not applicable	Not mentioned at all
1.6 Private meetings with the AC chairperson	Reported that CAE has private meetings with AC chairperson or other member	Not applicable	Not mentioned at all
2.1 Approval of IAA charter	Reported that the IAA charter is reviewed and agreed upon by the AC	The IAA charter is reviewed but not agreed upon by the AC	Not mentioned at all
2.2 Administrative reporting to CAE	Reported that the IAA reports administratively to the chief executive officer	The level to which the IAA reports administratively is reported, however, it is not to the chief executive officer	Not mentioned at all
2.3 Functional reporting to AC	Reported that the IAA reports functionally to AC	The level at which the IAA reports functionally is reported, however, it is not to the AC	Not reported at all
3.1 Appointment of CAE supported by the AC	Reported that the AC is involved in the appointment of the CAE	Reported that CAE was appointed but no mention of the involvement of the AC	Not mentioned at all
3.2 Dismissal of CAE supported by AC	Reported that the AC endorses the dismissal of the CAE	Reported that the CAE was dismissed but no mention of the endorsement of the AC	Not reported at all
3.3 Performance evaluation of the CAE	Reported that the AC evaluates the performance of the CAE	Reported that the CAE's performance was evaluated but no mention that it was evaluated by the AC	Not reported at all
3.4 Determination of the CAE's remuneration	Reported that the remuneration of the CAE is determined in consultation with the AC	Reported on remuneration of the CAE, but no mention was made of involvement of the AC	Not reported at all

The Southern African Journal of Accountability and Auditing Research

Evolving Research

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 20/10/2016

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. 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 electronically (selected hardcopies) distributed to a wide audience:

- authors of articles
- SAJAAR reviewers
- 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
- senior role players in South Africa's public sector
- subscribers (individuals and entities).
- SAIGA members

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 R342.00 per page (R300 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 2016). 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: 2016: R798.00 (R700 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 that was submitted originally (typed in double spacing).

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 reviewers, 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 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" if all authors are from the same institution. Alternatively invoices will be made out to all co-authors per institution and per contribution to the article. Proof of payment needs to be e-mailed 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.
(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 full payment of the invoice is his/her responsibility in the event that co-authors are not meeting their commitment towards the Institute. 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 ensure that the invoices are paid 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 – 2016-04-14*.

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 numbers and e-mail address 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 – 2016-04-14*.

3 The actual manuscript

The manuscript submitted for consideration must adhere to the following *technical standards*:

3.1 The manuscript must 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 The manuscript must 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 No footers or headers or other graphics, lines and blocks sometimes used to enhance documents (blocks around each page, etc.) may be included in the manuscript.
3.4 The manuscript must 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 The manuscript must 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 The text must be in English.
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 – 2015-11-01*. 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 – 2015-11-01.* Where more than two authors are involved use "et al" after first author. For example: *Smith et al – Accountability in the public sector – 2016-04-14.*

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 *admin@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 SAJAAR's editor (in chief) or secretariat.

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*. The form of the research award is monetary (accompanied by a certificate) of which the amount will be determined on an *ad* hoc basis by the Executive Committee of SAIGA. Articles published in *SAJAAR* are automatically considered for the *SAIGA Research Award*. A panel of international experts, comprising of academics and senior government auditors make a recommendation to the SAIGA Council 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 – 2016-04-14*.

5 Electronic submissions only

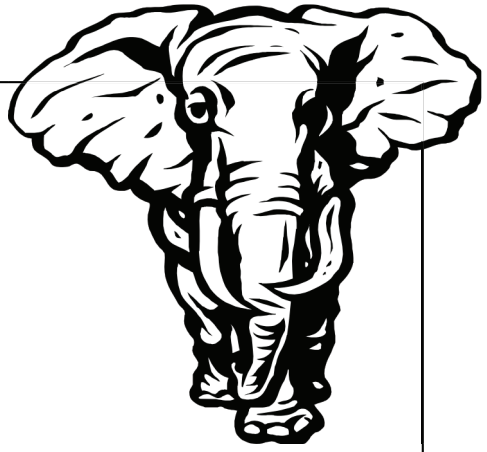
Submissions can only be done electronically. The submission must be e-mailed to *admin@saiga.co.za* and addressed to: The Editor, SA Journal of Accountability and Auditing Research.
No other e-mail address may be used.
File names must be constructed in the required file format.
Every submission must 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



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.

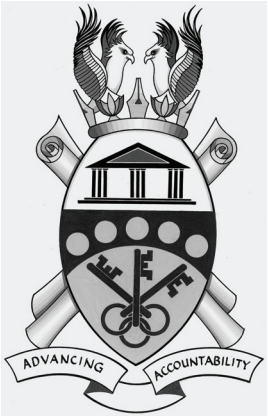
Our members' vision and determination helped develop Government Auditing to its current levels.

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.



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

SAIGA

ADVANCING AUDITING AND ACCOUNTABILITY

PO Box 36303 Menlo Park 0102 South Africa
Tel: 012-362-1221 Fax: 012-362-1418
www.saiga.co.za

Evolving Research

SAICA

ADVANCING AUDITING AND ACCOUNTABILITY