

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

T M Chikwiri

Department of Auditing
University of Pretoria

S P de la Rosa

Murray and Robberts

ABSTRACT

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

Key words

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

1 INTRODUCTION

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

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

implementation of internal audit strategies.

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

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

emphasise that the consequences of inadequate GRC are severe and can lead to insolvency – hence the necessary incongruity of increased spending on GRC functionality in a period of tightening budgets.

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

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

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

2 RESEARCH OBJECTIVES, SCOPE, METHODOLOGY, AND LIMITATIONS

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

Research approach

A qualitative approach was considered to be appropriate for this study, as it allows for deeper

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

Data collection

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

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

Research method

To achieve the aims of the research, a case study method was used in order to answer the "how" and

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

Population and sample size

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

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

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

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

Data analysis

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

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

Study limitations

This study aimed to understand, explore and explain the role of internal audit in the process of embedding GRC in SOCs. This study investigated the perceptions of CAEs and managers of GRC practices in their organisations, and of the role played by internal audit in the process. The first limitation of this study is inherent in the choice of research methodology, involving as it did the use of personal interviews, as the perceptions of interviewees on GRC may differ from practice. In addition, the sample was limited to only three SOCs out of a possible 21 major public entities in South Africa. Thus, it may not reflect the views of all CAEs in the South African SOCs environment, nor those of private sector CAEs, both

in South Africa and in other countries. However, it is probable that the outcomes would be similar if the study were conducted in the private sector as, according to commentary in the EY's Excellence in Integrated Reporting Awards 2013, SOCs and private sector entities alike are embracing the 'King Code of Governance Principles'. The second limitation is that the findings of this study are specific to the South African state owned company environment. The third limitation is that the SOCs selected for this study were drawn from the rankings produced for EY's Excellence in Integrated Reporting Awards 2013, and the methodology and processes used to rate SOCs for that purpose was not reviewed.

3 LITERATURE REVIEW

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

3.1 The GRC concept

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

Governance is:

- "...the combination of processes and structures implemented by the board to inform, direct, manage, and monitor the activities of the organization toward the achievement of its objectives" (IIA 2013).
- "...the arrangements put in place to ensure that the intended outcomes for stakeholders are

defined and achieved" (International Federation of Accountants 2014:5).

- "...the way organisations are directed and controlled" (Cadbury 1992; Pickett 2011:13).
- "...the ethical direction and control of an organisation to achieve its objectives while considering stakeholders needs and expectations" (IODSA 2009; Naidoo 2009:15).
- "...a set of relationships between a company's management, its board, its shareholders and other stakeholders and structures through which company objectives are set, attained and monitored" (OECD 2004:11).

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

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

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

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

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

and regulatory mandates and standards that govern the organisation”.

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

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

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

3.2 SOCs and their relevance in the South African context

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

public resources within SOCs has been attributed to poor GRC practices (PwC 2011:6).

3.3 State of GRC in SOCs

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

3.4 GRC Maturity Models

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

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

2012:8). The Aligned and Optimised Platform maturity levels indicate that GRC processes are increasingly integrated, as indicated by the presence of an entity-

wide GRC strategy with common GRC approaches, frameworks, and technology architecture, and the automatic sharing of information (Rasmussen 2012:8).

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

Level 1 Unaware	Level 2 Fragmented	Level 3 Integrated	Level 4 Aligned	Level 5 Optimised platform
<p>Governance, risk and compliance interdependencies are not understood by business.</p> <ul style="list-style-type: none"> • Approach to technology is ad hoc and technology is non-existent. • Risk and compliance information is managed in documents and spreadsheets. • Information is not available, let alone shared. • Success is not measured. • GRC components operate in isolation. Business management characterised by reactive and non-integrated approaches. • Redundancies are widespread. • Few if any resources are allocated to risk and compliance. • Risk and compliance issues are addressed in a reactive mode: assessments only performed when forced to. • There is no ownership or monitoring of risk and compliance, and certainly no integration of risk and compliance information and processes, even at the function level. • Risk, compliance and controls are documented and maintained only as-needed. • There is no trending or analytics to track the state of risk and compliance. 	<p>Limited understanding of governance, risk and compliance interdependencies; no common platform for GRC provided.</p> <ul style="list-style-type: none"> • Tactical, siloed approach to technology and systems, without integration. • There is some use of risk and compliance technology, but no integration or sharing of information and processes at function level. • The organization struggles with risk and compliance information that is trapped in silos' databases, spreadsheets and documents. • Measurement and trending is limited, consumes resources and takes a lot of time because of the scattered nature of risk and compliance information. • Approach not driven by risk. • Redundancy controls still minimal. • Relies on inefficient and labour intensive testing. • "Reactive" approach to managing control issues. • Risk and compliance is tactical and siloed (isolated) within the functions. • There is the beginning of accountability for risk and compliance. • Risk and compliance assessments are project-focused, not an ongoing effort of continuous monitoring. 	<p>The need to integrate GRC systems is recognised as the way to provide better information and results.</p> <ul style="list-style-type: none"> • Existence of a common GRC platform and approach at function level. • Integrated GRC approach has not yet expanded as a strategy across multiple functions. • There are defined processes and a single strategy for GRC at the business function level. • There is an integrated information architecture supported by appropriate technology, and there is ongoing reporting, accountability, and oversight for risk and compliance functions. • Risk and control "owners" are defined and held accountable. • Information is shared across the enterprise. • GRC benefits are measured. • There are established processes for and regular assessments of risk and compliance. • The business can readily trend, monitor and report on GRC at any time and across periods, without significant inefficiencies. 	<p>Governance, risk and compliance interdependencies are understood and aligned.</p> <ul style="list-style-type: none"> • There is a defined GRC strategy that crosses several or all GRC functions across the business. • Silos of GRC have effectively been eliminated, though there may remain some holdouts. • There is a common process, technology and information architecture supporting GRC across the business. • Business benefits are measured. • There is coordination of efforts to identify risks, assess exposure and prioritise actions. • Clear accountability and ownership of risk and control has been established across the organization. • The business is able to trend and report on GRC across all business functions. 	<p>A common language and set of metrics to continuously improve the GRC platform now exists.</p> <ul style="list-style-type: none"> • There is a cohesive GRC strategy that is integrated throughout the business. • GRC technology is fully integrated. • GRC is embedded in all business systems. • The GRC strategy is supported and understood by the board and executive management. • Complete visibility to risk exposure and performance. • Identification of GRC expectations is part of annual strategic planning process. • GRC is understood, measured, and monitored in the context of business performance, strategy and objective management. • Continuous measurement and monitoring of risk and compliance in the context of the business and performance is performed.

3.5 Embedding GRC in an organisation

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

of the entity's current maturity level, from which point the model can be used to direct management's strategy, processes, and action plans to achieve the preferred level of integration.

The process of embedding GRC (as with any business venture) starts with developing a strategy that includes clear objectives, goals, and vision (Frigo & Anderson 2009b:37). Thereafter, obtaining buy-in from the executive management and the board is vital (Proviti 2009:16; Anon 2011:39). Once a better understanding of GRC has been achieved by the board and senior management integration proceeds more efficiently and effectively because roles and

relationships are more clearly understood and defined (Raths 2011:19; Frigo & Anderson 2009a:6; Anon 2011:39). This also ensures that GRC is managed effectively, delivers the required stakeholder value and sustains profitability (Anand 2010:57). To coordinate the implementation of the strategy, the board must appoint a committee that is representative of all those affected by GRC implementation (Proviti 2009:16). The committee should act as the single reference point for GRC issues, which will ultimately reduce costs and enable the effective embedding of the GRC processes (Greengard 2011:23).

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

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

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

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

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

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

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

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

- Assist management to make a business case for GRC integration, by providing evidence on how the existing, individual components of GRC are already supporting business performance (albeit sub-optimally). This gives the internal auditors an

opportunity to better understand the organisation’s GRC processes. Steffee (2012:11) asserts that, through this process, internal auditors can improve their audit processes and bridge the gaps that exist between the GRC activities;

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

development (Frigo & Anderson 2009b:34). This also includes working together with executives to prioritise problems related to GRC implementation (Marks 2011).

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

4 RESULTS AND DISCUSSIONS

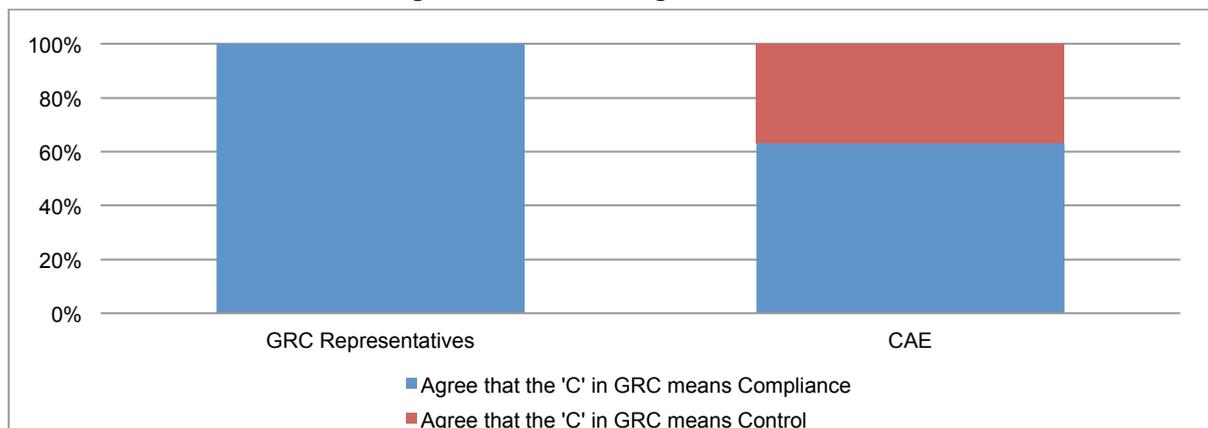
The results of the study will be analysed and discussed under the following subheadings:

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

Understanding the GRC concept

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

Figure 1: Understanding the ‘C’ in GRC

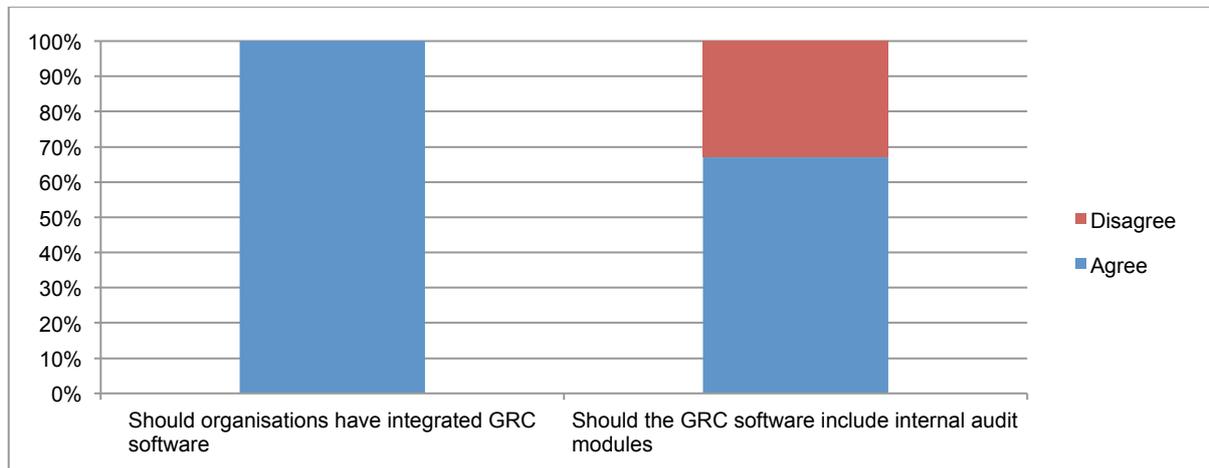


There was 100% consensus that GRC functions are there to ensure that businesses achieve their objectives. The GRC Project Manager for SOC A succinctly emphasised that to understand GRC, one first has to understand the value of each of the individual GRC functions before one can understand their collective value. 67% of CAEs held the view that everything starts with governance, as it is the key pillar for GRC. Governance is the umbrella concept within which risk management provides the key function. Compliance is a component of risk management, and all three aspects must be aligned. The CAE of SOC B stated that unless these three elements operate at a mature level an organisation would struggle to achieve its objectives. The results of the study indicate that 67% of CAEs and 100% of GRC representatives involved in GRC functions have the same understanding of GRC. The results of the study are in line with literature, as Proviti (2009:15); Frigo and Anderson (2009b:34); and McCleen, (as quoted by Raths 2011:19), state that having the same understanding on GRC principles clears barriers to effectively embedding GRC.

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

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

Figure 2: CAEs views on GRC software



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

internal audit module should be part of the integrated GRC software system.

GRC maturity level in the selected SOCs

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

The CAEs for SOCs B and C confirmed that the maturity levels for their entities are between "fragmented" and "integrated". SOC A's CAE and the GRC Project Manager have different understandings of their SOC's GRC maturity level. The CAE sees it as "integrated" while the GRC Project Manager views it as falling between "fragmented" and "integrated". The differing perspectives on GRC maturity stages expressed by internal auditors and those with GRC management responsibilities suggests that a full embedding of GRC is yet to take place in SOCs. This also supports the view that within an organisation one element of the GRC functions might well be "mature,"

while the others are still only “evolving”. The CAE for SOC B was unusually specific, stating that their maturity level was 75% “fragmented” and 25% “integrated,” while SOC B’s GRC representative’s view was that it was “integrated”. The differing views within the same organisation show that GRC is not fully embedded in this entity. There was consensus amongst all interviewees that the GRC maturity level for SOCs in general is still “fragmented”. The inference is that within SOCs, GRC is still seen as three individual functions and not as an integrated whole. Although SOCs A and C have executives

dedicated to overseeing all GRC functions, their maturity levels are still between “fragmented” and “integrated”. The GRC Project Manager for SOC A stated that, while their GRC functions are effective individually, what is lacking is the integration of these siloed functions that would enable the organisation to develop a holistic business perspective on risk and compliance. The results of the study are in line with the views put forward by Hoon (2011:22) and Anderson (2011:60), that the current GRC processes in organisations is still best described as ‘fragmented’ and needs to evolve.

Table 2: GRC maturity levels of SOCs

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

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

Embedding GRC and the role played by internal audit

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

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

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

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

In addition to generally agreeing with the above,

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

In addition, SOC C’s CAE explained that the internal auditors play an active role in embedding GRC functions in the organisation through spearheading meetings of the combined assurance steering committee. Obstacles to the embedding of GRC processes are identified and addressed by the combined assurance steering committee at these meetings. Effectively, the coordination of the efforts of the

constituent functions of the combined assurance model results in GRC processes being embedded. SOC B's CAE stated that their internal audit function influences the process of embedding GRC functions, in line with the generally accepted combined assurance model, by being represented at every executive and operational committee level within the organisation.

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

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

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

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

The CAEs in SOCs B and C, and SOC A's GRC Project Manager each acknowledged that internal audit is able to assist their organisations to move to a

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

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

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

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

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

processes and systems is critical to the overall success of GRC (Chartis Research Ltd 2014:5).

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

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

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

5 CONCLUSION

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

executive support, difficulty in achieving agreement on key definitions, and the choice of technology.

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

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

REFERENCES

- Abdolmohammadi, M.J., Ramamoorti, S. & Sarens, G. 2013. *CAE Strategic Relationships: Building rapport with the executive suite*. The Institute of Internal Auditors Research Foundation. Altamonte Springs, Florida.
- Anand. S. 2010. Technology and the Integration of Governance, Risk Management and Compliance. *Financial executive*, December, 12:57-58.
- Anderson. S. 2011. Automating governance, risk and compliance. *Financial Executive*, 27(5):60-63.
- Anon. 2010. US insurers taking up GRC in budget drive. *Operational Risk & Regulation*, 11(7):29.

- Anon. 2011. Pushing for GRC. *Operational Risk & Regulation*, 12(7):38-41.
- Balachandran, B.V. & Sundar, K.S. 2013. Governance, risk, and compliance: The value driver for good corporate governance. *Cost Management*, 27(6):39-47.
- Batenburg, R., Neppelenbroek, M. & Shahim, A. 2014. A maturity model for governance, risk management and compliance in hospitals. *Journal of Hospital Administration*, 3(4):43-52.
- Bloomberg, L.D. & Volpe, M. 2012. *Completing your qualitative dissertation – A road map from beginning to end*. 2nd edition. Sage Publications. Los Angeles.
- Boulton, B. 2013. *The GRC value proposition*. Global Association of Risk Professionals. [Online]. www.garp.org/risk-news-and.../the-grc-value-proposition.aspx (Accessed: 6 January 2014).
- Bouwman, N. 2010. Governing state-owned enterprises. *Without prejudice*, December, 10(11):26-28.
- Cadbury Report, A. 1992. *Report of the committee on the financial aspects of corporate governance*. The Committee on the Financial Aspects of Corporate Governance. Gee and Company Limited. London.
- Carpenter, B. 2012. Award-Winning GRC. *Internal Auditor*, August, 69(4):17.
- Chambers, R.F. 2014. *Lessons learned on the audit trail*. The Institute of Internal Auditors Research Foundation. Altamonte Springs, Florida.
- Chartis Research Ltd. 2014. *Enterprise GRC Solutions 2014: Time for GFRC?* MetricStream Vendor Highlights. [Online]. <http://www.chartis-research.com> (Accessed: 7 July 2014).
- Coetzee, G.P. 2010. *A risk-based audit model for internal audit engagements*. Unpublished PhD thesis in Auditing. Bloemfontein: University of the Free State.
- Committee of Sponsoring Organisations of the Treadway Commission (COSO). 2004. *Enterprise risk management integrated framework: Executive summary*. Sponsoring Organisations of the Treadway Commission. Jersey City. New Jersey.
- Companies Act no 71 of 2008. Pretoria: Government Printers.
- Creswell, J.W. & Clark, V.L.P. 2007. *Designing and conducting mixed methods research*. Thousand oaks, CA: Sage.
- Davis, S. & Lukomnik, J. 2010. Enabling good governance. *Internal Auditor*, April, 67(2):28-29.
- Ernst & Young. 2013. EY's Excellence in Integrated Reporting Awards 2013. *A survey of integrated reports from South Africa's top 100 JSE listed companies and top 10 state owned companies*. [Online]. [http://www.ey.com/Publication/vwLUAssets/EYs_Excellence_in_Integrated_Reporting_Awards_2013/\\$FILE/EY%20Excellence%20in%20Integrated%20Reporting.pdf](http://www.ey.com/Publication/vwLUAssets/EYs_Excellence_in_Integrated_Reporting_Awards_2013/$FILE/EY%20Excellence%20in%20Integrated%20Reporting.pdf) (Accessed: 17 March 2014).
- Fraser, I. & Henry, W. 2007. Embedding risk management: structures and approaches. *Managerial Auditing Journal*, 22(4):392-409.
- Frigo, M.L. & Anderson, R.J. 2009a. Strategic Framework for Governance, Risk, and Compliance. *Strategic Finance*, February, 90(8):20-61.
- Frigo, M.L. & Anderson, R.J. 2009b. 10 Strategic GRC: Steps to implementation. *Internal Auditor*, June, 10:33-37.
- Greengard, S. 2011. The GRC Maze. *Baseline*, September/October, 112:20-24
- Hoon, A. 2011. A holistic approach to GRC. *Accounting Today*, 25(7):22-25.
- Institute of Directors Southern Africa. 2009. *King Report on Governance for South Africa*. Johannesburg. Institute of Directors Southern Africa.
- Institute of Risk Management, UK. 2002. *A Risk Management Standard*. [Online]. http://www.theirm.org/publications/documents/Risk_Management_Standard_030820.pdf (Accessed: 10 July 2010).
- International Federation of Accountants (IFAC). 2014. *International Framework: Good Governance in the Public Sector – Supplement*. [Online]. <https://www.ifac.org/sites/default/files/publications/files/International-Framework-Good-Governance-in-the-Public-Sector-supplement-IFAC-CIPFA-June-2014.pdf> (Accessed: 7 July 2014).
- International Standards Organisation. 2009. *ISO 31000: Risk Management – Principles and Guidelines*, ISO. Geneva, Switzerland.

- Konstans, C., Radhakrishnan, S., Switzer, C.S. & Williams, L.C. 2011. In search of 'principled' performance. *Financial Executive*, 27(10):55-57.
- KPMG.2007. *The evolving role of internal audit: Value creation and preservation from an internal audit perspective*. [Online]. <https://www.kpmg.com/ZA/en/IssuesAndInsights/ArticlesPublications/Risk-Compliance/Documents/The%20Evolving%20role%20of%20the%20Internal%20Auditor.pdf> (Accessed: 7 June 2014).
- KPMG. 2012. *A good offense is the best offense: Managing regulatory compliance with GRC*. [Online]. <https://www.kpmg.com/US/en/IssuesAndInsights/ArticlesPublications/Documents/managing-regulatory-compliance-grc.pdf> (Accessed: 7 June 2014).
- Lamont, J. 2012. GRC: The upside of risk. *KMWorld*, October, 21(9):18-19
- Marks, N. 2010. Defining GRC. *Internal auditor*, February:25-27.
- Marks, N. 2011. *The GRC Survey: The results are in*. [Online]. <http://normanmarks.wordpress.com/2011/02/01/the-grc-survey-the-results-are-in/> (Accessed: 23 July 2014).
- McGraw, S. 2012. GRC focus: Keep your employees close and your auditors closer. *Compliance & Ethics Professional*, (March/April):28-29.
- Meiselman, J. 2007. Risk, Governance and compliance trends for 2007. *Risk Management*, 54(2):40.
- Metricstream. 2013. *The Future: Pervasive GRC*. [Online]. <http://www.metricstream.com/pdf/whitepapers/Pervasive-GRC.pdf?alid=105897079> (Accessed: 6 January 2014).
- Mitchell, S.L. & Switzer, C.S. 2009. *GRC Capability Model*. Red Book 2.0. Open Compliance & Ethics Group, Phoenix.
- Municipal Finance Management Act (MFMA). 2003. *Act No 56 of 2003*, Pretoria: Government Printers.
- Naidoo, R. 2009. *Corporate governance: An essential guide for South African Companies*. 2nd edition. Durban: LexisNexis.
- National Treasury of South Africa. 2010. *Public Sector Risk Management Framework*. Pretoria: Government Printers.
- Nissen, V. & Marekfa, W. 2014 The Development of a Data-Centred Conceptual Reference Model for Strategic GRC. *Management. Journal of Service Science and Management*, 7:63-76.
- Nkonki Incorporated (Nkonki). 2013. *Insights into SOC* Integrated Reporting Trends in South Africa*. [Online]. <http://www.nkonki.com/IR/publications.php?a=integrated-reports&page=insights-into-soc-integrated-reporting-trends-2013> (Accessed: 27 July 2014).
- Organization for Economic Co-Operation and Development (OECD). 2004. *Principles of Corporate Governance*. [Online]. <http://www.oecd.org/corporate/ca/corporate/governance/principles/31557724.pdf> (Accessed: 3 July 2014).
- Phalke, V. 2009. Breaking down silos for integrated Governance, Risk and Compliance. *Siliconindia*, February:39.
- Pickett, K.H.S. 2011. *The essential guide to internal auditing*. 2nd edition. West Sussex: John Wiley & Sons.
- Protiviti. 2009. *Key questions surrounding integrated GRC*. [Online]. http://www.protiviti.com/en-US/Documents/White-Papers/Risk-Solutions/Integrated_GRC.pdf (Accessed: 30 June 2014).
- Protiviti. 2013. *Growing with Governance, Risk and Compliance (GRC) Solutions. Avoiding common pitfalls to maximise GRC solutions*. [Online]. <http://www.protiviti.com/en-US/Documents/White-Papers/Risk-Solutions/Growing-With-GRC-Solutions-Protiviti.pdf> (Accessed: 4 July 2014).
- PricewaterhouseCoopers (PwC). 2011. Stated-owned enterprises: *Governance responsibility and accountability. Public Sector Working Group: Position Paper 3*. [Online]. http://c.ymcdn.com/sites/www.iodesa.co.za/resource/collection/879CAE6C-7B90-49F5-A983-28AECBCE196F/PSWG_Position_Paper_3_Governance_in_SOEs.pdf (Accessed: 30 June 2014).
- Public Finance Management Act (PFMA). 1999. *Act No 1 of 1999*, Pretoria: Government Printers.
- Rasmussen, M. 2009. An Enterprise GRC Framework. *Internal Auditor*, October, 10:61-65.
- Rasmussen, M. 2012. GRC Maturity: *From Disorganized to Integrated Risk and Performance*. Corporate Integrity, LLC. [Online]. <http://grc2020.com/2012/04/20/57grc-maturity-from-disorganized-to-integrated-risk-and-performance/> (Accessed: 31 July 2014).

- Raths, D. 2011. The big picture. *KM World*, 20(7):18-19.
- Stanford, J. 2004. Curing the ethical malaise in corporate America: Organizational structure as the antidote. *Sam Advanced Management Journal*, 69(3):14-21.
- Steffee, S. 2012. GRC Conundrum. *Internal Auditor*, 69(2):11-13.
- Steinberg, R.M. 2010. Common Questions about GRC and Some Answers. *Compliance Week*, September: 40-41.
- Tadewald, J. 2014. GRC Integration: A conceptual Foundation Model for Success. *Management accounting quarterly*, Spring 2014, 15(3):10-18.
- Teddlie, C. & Yu, F. 2007. Mixed Methods Sampling: A Typology With Examples. *Journal of Mixed Methods Research*, 1:77, SAGE publications.
- The Institute of Internal Auditors (IIA). 2013. *International Professional Practices Framework*. Altamonte Springs, FL, from the glossary.
- The Institute of Internal Auditors Research Foundation (IIARF). 2013. *Contrasting GRC and ERM: Perceptions and Practices among Internal Auditors*. [Online]. <http://www.theiia.org/bookstore/product/contrasting-grc-and-erm-perceptions-and-practices-among-internal-auditors-download-pdf-1751.cfm> (Accessed: 17 June 2014).
- The Risk Management Institution of Australasia Limited (RMIA). 2012. *The role of the risk professional in leading the G in GRC*. [Online]. <http://www.rmpartners.com.au/images/stories/Whitepapers/Risk%20Professionals%20Leading%20the%20G%20in%20GRC.pdf> (Accessed: 7 June 2014).
- Thomson Reuters Accelus. 2012. Building a business case for governance, risk and compliance. [Online]. www.accelus.thomsonreuters.com/sites/default/files/GRC00015.pdf (Accessed: 9 August 2014).
- Verschuren, P. & Doorewaard, H. 2010. *Designing a research project*, 2nd edition, The Hague: Netherlands.
- Yin, R.K. 2009. *Case study research: Design and methods*, 4th edition. London: Sage Publications.

