Journal of Contemporary Management
Volume 13

Enterprise risk management at South African state-owned companies

H VERGOTINE

Department of Industrial Psychology and People Management,
University of Johannesburg

vergotineh@arc.agric.za

A THOMAS *

Department of Industrial Psychology and People Management,
University of Johannesburg

*adelet@uj.ac.za * Corresponding author*

Abstract

State-owned companies play a central role assisting governments to promote the well-being of citizens in developing countries. As such, they must be well governed. Integral to sound governance is an holistic strategy to ensure that risk is managed.

The objective of the present qualitative study was to identify those components of risk that could be incorporated into Enterprise Risk Management (ERM) at South African state-owned companies. The first part of the study entailed a document review at seven Schedule 2 state-owned companies. The second part of the study involved a Delphi survey with 18 expert risk managers in the public sector.

From a combination of the findings of parts 1 and 2, five main themes emerged as being important for consideration when addressing risk at state-owned companies. The study provides pointers for consideration in the endeavour to incorporate ERM as an integral part of strategic and operational processes at state-owned companies.

Key phrases

Delphi survey; developing countries; governance, qualitative study

1. INTRODUCTION

One of the main contributing factors to the global financial crises over the years has been the widespread lack of risk management by both financial and non-financial organisations (Lundqvist 2015:442). In spite of the importance of risk management, current measurements for assessing risk management are based on either subjective assessments or appear to be checklists of activities based on subjective opinions (Coetzee & Lubbe 2013:46; Kimbrough & Componation 2009:22; Lundqvist 2015:442).

Thusfar, little research has been conducted on risk management in South African state-owned companies (SOCs) that contribute substantially to the Gross Domestic Product of developing countries and often play prominent roles in the energy, transportation, and telecommunications industries (OECD 2005:11).

Overall, 715 SOCs service various social and commercial initiatives across all spheres of the South African economy (Republic of South Africa 2011:67). Of this number, 21 SOCs are classified as Schedule 2 major public entities. These major SOCs contribute substantial financial, investment, labour, technology, and infrastructure resources, and are dominant across sub-Saharan Africa's transport, freight logistics, communication, energy, and defence-related sectors (Republic of South Africa 2015:22). Seven of the major 21 SOC's had a collective capital investment estimated to be in excess of R86 billion in the 2014/2015 financial year (South African Government Communication and Information System 2015:3).

The importance of the strategic role played by SOCs in the well-being of all citizens and in the competitiveness of private sector companies and industries, led the OECD (2005:12) to develop guidelines for the governance of SOCs. These guidelines detail the core elements of good corporate governance practices for SOCs and are considered to be the first international benchmark used to evaluate and improve government's ownership role as the major shareholder in these entities (OECD 2015:11).

2. PROBLEM INVESTIGATED

The Auditor General of South Africa (AG-SA) (2011:51) found that 69% of SOCs do not comply with regulatory requirements related to risk management, 51% do not maintain

effective risk management strategies, and 61% lack business continuity and disaster recovery plans. Subsequent reporting by the AG-SA (2013:54; 2014:70) indicates that the overall governance processes in the public sector have shown little improvement over the years; the level of risk assurance provided by senior management in the public sector has declined to a low base of 35% at the level of Accounting Officers/Authorities and 30% at the level of Executive Authorities. Coetzee and Lubbe (2013:50) report that, while South African private sector organisations are mostly risk mature, public sector organisations are severely lacking in this respect.

Given this background, the findings of the present study aim to assist leaders of South African SOCs in considering those components of risk management that must be incorporated into business and thus advance the execution of the mandate of SOCs in a developing country.

3. OBJECTIVE OF THE RESEARCH

The overall objective of the study was to identify those components of risk that can be considered for incorporation into Enterprise Risk Management (ERM) at South African SOCs.

The sub-objectives were to:

- identify practices of risk management at selected SOCs as evidenced in internal documentation;
- ascertain the views of risk management experts about the components of risk management that should be addressed at SOCs;
- combine the identified practices noted in the SOC documents with that provided by the expert input into suggested pointers for consideration for ERM at South African SOCs.

4. THEORETICAL BACKGROUND

4.1 Corporate governance

Corporate governance is “the system by which companies are directed and controlled” (Cadbury 2000:9) and aims to influence the systems and processes relating to the power

and control over the organisation's direction, behaviour, and performance (Monks & Minow 1995:6). Such influence, accordingly, assures investors of the sound governance of their assets (Mande, Park & Son 2012:195; Shank, Hill & Stang 2013:385) and integrates the interests of shareholders, customers, employees, and the public (Hilb 2005:570).

Organisations such as the World Bank and the International Finance Corporation have provided loans linked to corporate governance principles in order to ensure that governments and private sector companies raise their governance standards to globally acceptable levels (Balgobin 2008:18).

The management of risk falls within the ambit of corporate governance. Organisations are encouraged to develop risk-based internal audits that incorporate strategic direction with written assessment to boards of directors detailing the adequacy and effectiveness of internal controls (Beasley, Clune & Hermanson 2005:530; Buehler Freeman & Hulme 2008:105).

4.2 The management of risk

4.2.1 The importance of risk management

Market uncertainty and increased stakeholder pressure has forced companies to manage risk in the planning, controlling, and execution of business processes (Lundqvist 2014:393; Yaraghi & Langhe 2011:551). Accordingly, the management of risk has become a strategic business imperative, with CEOs placing increasing emphasis on the management of all types of risks (Heiligtag, Schlosser & Stegmann 2014:6).

Corporate scandals have highlighted the need for boards of directors to assess a wide range of risk within environments of growing regulatory interventions, and ones in which institutional investors regard robust risk management processes as constituting a worthy cost of business (Lundqvist 2014:394). In addition, South African CEOs and boards of directors, increasingly, are expected to take ownership of managing company risk as outlined, in particular, in the King Report on Corporate Governance (IOD 2009:14). However, there is still a lack of consensus on models of risk management and on the application of

extant models in business (Oliva 2016:66) In addition, the description of many concepts is vague (Bromiley, McShane, Nair & Rustambekov 2015:268).

4.2.2 Requirements for successful risk management

The success of risk management depends on the existence and usefulness of a management framework that lays the foundation for embedding the process across the organisation (Yaraghi & Langhe 2011:576). Traditional risk management involves identifying, measuring, monitoring and reporting on risk with little formality, structure or centralisation (Lundqvist 2015:442). However, the management of risk has evolved from a traditional silo-based approach, i.e. risk control and insurance practices combined within operational activities, to the assessment of potential risk exposures and the impact that such exposures could have across all business activities of an organisation (Van Wyk, Dahmer & Custy 2004:260).

This non-silo-based approach, known as ERM (Lundqvist 2015:443), is a process endorsed across an organisation and applied in the development of organisational strategy (Committee of Sponsoring Organizations of the Treadway Commission [COSO] 2004:13; Lam 2014:51). It equates to integration (Bromiley *et al.* 2015:265) and links strategic objectives and organisational growth opportunities to potential risk exposure (Bromiley *et al.* 2015:268; Kleffner, Lee & McGannon 2003:54) as well as identifies risk factors in a business, assesses the severity of such risk, quantifies its magnitude, and mitigates the exposure (Stroh 2005:28).

ERM is a systematic approach that aims to assess and manage all sources of risks that could negatively influence the accomplishment of organisational objectives (Lai, Azizan & Samad 2010:25) and includes uniting an organisation's internal procedures with its external risk environment in order to optimise the organisation's return on investments (Drew & Kendrick 2005:26). Put another way, ERM involves the "direction and control" of an organisation's risk management system in which responsibilities, authority and accountability are delineated, and rules and procedures for decision-making are specified (Lundqvist 2015:442). Bromiley *et al.* (2015:265) suggest that ERM demands that organisations

address risks in a comprehensive and coherent manner and that there is alignment of risk management between corporate governance and the strategy of organisations.

4.2.3 Enterprise risk management

There are four risk management requirements that comprise the platform from which the ERM process is developed (Leitch 2010:888).

First, a risk management policy that is relevant to the strategic objectives, goals, and the nature of an organisation's activities must be developed. While traditionally identified risks such as product liability must be taken into account, ERM demands that strategic risks such as competitor behaviour is also identified (Bromiley *et al.* 2015:268).

Second, planning and resourcing that outlines management's commitment, the assigning of responsibilities and authorities, and the identification and allocation of adequate resources to sustain and support the risk management process must be delineated.

Third, the processes involved in the implementation of the risk management programme must be addressed.

Fourth, management reviews and periodic reviews of the risk management programme to assess its suitability and effectiveness must be instituted.

Similarly, Lundqvist (2014:412) proposes that there are four discrete components of ERM: the general internal environment and objective setting, the general control activities, information and communication, the holistic organisation of risk management, as well as the specific identification of risk and risk assessment activities.

Lundqvist (2014:393) notes that ERM is the state that exists when all four interrelated components are present and functioning soundly. Within the unique context of the organisation, an holistic risk management framework should incorporate a combination of structures, processes, systems, methodology and people (those involved in orchestrating the risk management strategy) (Coetzee & Lubbe 2013:45).

The internal environment and the organisational culture are the bedrocks of the ERM process and, therefore, influence how organisations set their strategic objectives and adopt risk management processes (O'Donnell 2005:178). Lundqvist (2015:442) notes that the

governance of risk involves instilling a culture of risk-awareness throughout the organisation that is supported by organisational structure and formal governance mechanisms. In this regard, the commitment by leadership to risk management is one of the main determinants of an effective risk management strategy (Coetzee & Lubbe 2013:51). In addition, the internal environment also influences internal control activities, the communication of ERM matters and the monitoring of ERM processes.

The components of the internal environment include: the risk management philosophy, the setting of a risk appetite level, the role of the board of directors, the organisational structure, and the assignment of ERM authority and responsibilities (COSO 2004:27).

Holistic ERM should combine traditional risk management processes as well as risk governance which relates to the manner in which risk management is organised (Lundqvist 2015:442). Such risk governance has been found to related positively to organisational performance (Aebi, Sabato & Schmid 2012:3224; Baxter, Bedard, Hoitash & Yezegel 2013:1291).

4.2.4 Risk maturity

Central to risk management is the assessment of exposure to risk and the risk maturity of the organisation. Hillson (1997:35) proposes a method to calculate risk based on three specific pressure point clusters. In the growth pressure point cluster, areas that must be evaluated within organisations include pressure for performance, rate of organisational expansion and the inexperience of key employees. Within the cultural pressure point cluster, consideration must be given to the rewards offered for entrepreneurial risk-taking, executive resistance to bad news and the level of internal competition. In the information management cluster, transaction complexity and velocity, gaps in diagnostic performance management and the degree of decentralised decision-making, must be evaluated.

Quantifying risk exposure in this way assists in plotting the organisation on a continuum of safety, caution and danger. Organisations in the danger zone are exposed to risks that are unacceptable, unsafe, and ones that require urgent action, i.e. immediate resource allocation to minimise the resultant impact posed by the risks.

The risk management maturity model has four levels of process maturity (Risk Management Research and Development Program Collaboration 2002:6). Each level is linked to specific attributes that provide a methodology that allows a determination to be made whether or not organisational risk processes are adequate. Maturity levels are identified by assessing organisational attributes in relation to culture, processes, experience, and application. These attributes are evaluated by assessing commitment to perform (policies and leadership), ability to perform (resources and training), activities performed (implementation plans and procedures), measurement and analysis (measures and status), and verification (oversight and quality assurance).

The analysis positions the organisation in one of the four tiers of risk management maturity, namely *ad hoc*, initial, repeatable, and managed or in Hillson's (1997:36) terms, naïve, novice, normalised and natural, respectively. Organisations at the *ad hoc* level are deemed to be unaware of the need to manage their risks and, as a result, there is no structured approach to dealing with uncertainties that may negatively impact organisational operations. On the initial level, organisations experiment by applying risk management principles in specific areas but with no structured, widespread application across the organisation. Organisations in the repeatable level have applied risk management to routine business processes in combination with the development and rollout of generic risk policies and procedures.

At the managed level, organisations have established a risk-aware culture that advocates a proactive approach to the management of risks in all business processes. Risk mature companies have been found to demonstrate stronger financial performance than those that are less risk mature and evidence the permeation of risk management throughout major organisational processes (Oliva 2016:68;78).

While leaders of many organisations have expressed a heightened interest in ERM, its actual implementation is low (Heiligtag *et al.* 2014:3). A failure to assign dedicated resources to support the ERM process and a lack of understanding of the value that the process can contribute to an organisation, has resulted in a low level of ERM implementation in organisations (Ernst & Young 2006:9).

4.3 The management of risk within SOCs

Notwithstanding the practical differences between private organisations and SOCs, commonalities do exist in respect of their risk exposure categories. These commonalities suggest that the process for managing risk at SOCs is no different to that which applies to private sector companies (Fone & Young 2000:18).

This notion is further supported by the development of global, generic risk management principles that systematically and uniformly aid all organisations, both public and private, in managing their exposure to risk (COSO 2004:3; International Standards Organisation 31000 2009:1; Standards Australia and Standards New Zealand 2004:1).

The management of risk in the public sector is a general management function applicable to all managers and aimed at supporting government imperatives to promote socio-economic advancement (Fone & Young 2000:40). There is growing interest amongst public sector managers regarding the management of risk due to public demand for well-run government operations that achieve social and economic objectives and which avoid financial losses (Del Bel Belluz 2002:40).

Corporate governance standards pertaining to SOCs and legislative requirements that regulate the use of public funds have placed pressure on SOCs to develop effective, efficient, and transparent systems of risk management (IOD 2009:14; OECD 2005:7; Republic of South Africa 1999:57).

Risk in the SOC environment is never stable. New developments that include addressing infrastructural growth within budget, embracing technological change involving organisational cultural shift and greater complexity, ensuring thorough auditing processes and working leaner, all bring with them organisational and people risks (Piper 2014).

Emanating from the literature review, the major research question that this study sought to answer was: What are the major components of risk that can be considered for incorporation into Enterprise Risk Management (ERM) at South African SOCs? Given that risk management models differ (Oliva 2016) and that little research could be found regarding risk management at SOCs, this study sought to address this gap.

5. RESEARCH METHODOLOGY

This qualitative study was divided into two phases. Phase 1 dealt with the collation, analysis and interpretation of all relevant documentation relating to risk management at seven selected SOCs. In Phase 2, a Delphi survey was used, involving 18 risk experts at the seven SOCs and other public sector institutions. All organisations participating in the study as well as all participants were assured of confidentiality of responses. Accordingly, SOC names are only mentioned when the sample is noted. When the findings are presented and discussed, the field in which the SOC is located is used as the descriptor.

5.1 Phase 1: Population and sample

The population of SOCs comprised all 21 Schedule 2 SOCs (Republic of South Africa 2010:1-2) from which seven stratified and purposefully selected SOCs were chosen. The selection of SOCs was based on SOC dominance across sub-Saharan Africa, the value of assets, and shareholder reporting responsibility to the Department of Public Enterprises (Republic of South Africa 2010:1-2). The asset values of the SOCs are noted in Table 1.

Collectively, the total asset value of these seven SOCs is R770.8 billion. These seven SOCs were selected from the 21 SOCs in terms of their sub-Saharan dominance, the value of their assets and their accountability directly to the Department of Public Enterprises. They also span important areas that impact development in South Africa – diamond mining, the provision of infrastructure for telecommunications, the provision and maintenance of equipment used by the country's defence force, the generation of the country's electricity, the growing of timber and its processing, the local, regional and intercontinental operations relating to the delivery of freight and mail and passenger transport services, and focused freight transportation.

The above-mentioned services are essential to the efficient running of the economy and to the overall development of the country. They also contribute to the Gross Domestic Product of the country.

TABLE 1: Asset values of the selected SOCs

SOC	Core business	Asset value (R' billion)
Alexkor	Diamond mining	0.9
Broadband Infraco	Provision of telecommunication infrastructure to promote telecommunication market efficiency	1.6
Denel	Provision and maintenance of equipment for the South African National Defence Force	8.0
Eskom	Electricity generation	504.9
SAFCOL	Timber harvesting and processing	0.1
SAA	Operation of domestic, regional and intercontinental scheduled services for passengers, freight and mail	15.2
Transnet	Focused freight transportation	240.1
TOTAL		770.8

Source: Adapted from Republic of South Africa 2015:22

5.2 Phase 1: Data collection and analysis

At all SOCs, the following reports were interrogated to assess risk management strategies: corporate and strategic plans, shareholder compacts, monthly and quarterly reports, annual reports, ERM and materiality statements as well as significance frameworks. This was achieved through a content analysis of the reports where themes were identified and clustered.

According to McCulloch (2004:4), there is widespread neglect of and ignorance about the use of documents in research, in favour of considering only documents produced during the research study itself, such as interview guides and questionnaires. However, various authors (cf. Corbetta 2003:296; Flick 2009:293; Prior 2003:5) have found original documents to be central to, and of equal value in, research.

Similarly, Merriam (2002:13) notes that documents provide insights and clues, and are easy to locate and examine. Rapley (2007:111) indicates that documents are instructive in understanding organisational realities and also useful when used in combination with other collated data.

5.3 Phase 2: Population and sampling

Twenty-one risk experts were purposefully sampled to participate in a Delphi process. These participants included 17 risk practitioners from the seven SOCs, two representatives from the Department of Public Enterprises, and two representative from the forestry/agricultural sector as detailed in Table 2.

TABLE 2: Delphi experts approached

Industry sector	Number of experts approached
Energy	5
Defence	1
Aviation	4
Nuclear energy	1
Freight, pipeline, and port operations	4
Mining	1
ICT	1
Forestry and agriculture	2
Government (Department of Public Enterprises)	2
TOTAL	21

Source: Derived from SOC senior employee lists

The participants were purposively selected on the basis of occupying senior risk management positions as well as their involvement in the development, monitoring and review of ERM programmes. Accordingly, it could be expected that they would provide broad and meaningful comment on the issues under investigation.

5.4 Phase 2: Data collection and analysis

A three-round electronic Delphi survey was used to solicit responses from 18 of the targeted 21 experts who ultimately agreed to participate in the study. The Delphi technique (the Delphi) is a series of chronological questionnaires or rounds of questionnaires, combined with controlled feedback that aims to obtain a reliable consensus from a group of experts (Linstone & Turoff 1975:28), considered useful when individual judgements are required (Delbecq, van de Ven & Gustafson 1975:11).

The findings are combined in order to address a possible lack of agreement amongst experts or when an incomplete state of knowledge exists. The Delphi is widely used in business, industry, and healthcare research as an instrument that is useful for determining a collective level of truth amongst its participants (Linstone & Turoff 2002:4-5) and should typically consist of three rounds of questionnaires sent to a preselected panel of experts (Powell 2002:378).

Table 3 details the extent of participant involvement in the three Delphi rounds.

In Round 1, participants were requested to identify the components of ERM to be considered when assessing ERM processes. The results obtained from Round 1 were subjected to an inductive comparison analysis that led to the establishment of themes representing the identified ERM components. Round 2 entailed participants reaching consensus on the ERM themes that emanated from Round 1, and ranking the themes according to their perceived levels of importance. In Round 3, participants were provided with feedback about the results from the preceding two rounds, and were asked whether they agreed with the conclusions. They were afforded the opportunity to effect any changes and, thereafter, the Delphi survey was closed.

Eighteen experts agreed to participate in the survey with 15 completing Round 1 and 10 completing each of Rounds 2 and 3. All participants were assured of the confidentiality of

their responses and no identifying information was requested. Participation in the study was voluntary. Participants were offered access to the findings, should they so desire, in recognition of their participation in the study.

TABLE 3: Participant involvement in the Delphi rounds

SOC SECTOR	Original number of participants targeted	Participants who agreed to participate	Round 1 participants	Round 2 participants	Round 3 participants
Energy	5	5	3	2	2
Defence	1	1	1	1	1
Aviation	4	4	4	3	3
Nuclear energy	1	1	1	0	0
Freight, pipeline & port operations	4	3	2	1	1
Mining	1	0	0	0	0
ICT	1	1	1	0	0
Forestry & agriculture	2	2	2	2	2
Government	2	1	1	1	1
TOTAL	**21**	**18**	**15**	**10**	**10**

Source: Calculated from survey results

6. FINDINGS

6.1 Phase 1: Document analysis

The content analysis of documents revealed that there were several common ERM assessment processes identified across the SOCs that included ERM methodologies and frameworks, ERM governance structures, and ERM processes. All the SOCs had adopted one of the following three globally accepted ERM methodologies and frameworks: Standards Australia and Standards New Zealand (2004:11), the COSO (2004:23), the ISO 31000 Risk Management Standard (International Standards Organisation (ISO) 2009:9) and certain aspects of the locally accepted practices recommended by Institute of Risk Management South Africa Code of Practice (IRMSA 2004:20).

These methodologies and frameworks were used exclusively, in combination with each other, or in combination with other, similar business improvement methodologies, for example, quality management standards and balanced scorecards. As a result of the application of these ERM frameworks, the boards of directors of all seven SOCs had established various governance structures to monitor the process of risk management across all levels of the organisations.

In addition, the SOCs had adopted ERM processes that aimed at identifying, monitoring, and updating the risks faced by their organisations. The top ten risks to which the SOCs were exposed were updated on a regular basis. Various crosscutting risks, identified across the SOCs, included: inadequately trained staff, insufficient funds, ineffective execution of capital projects, the negative impact of the regulatory environment, and non-compliance with legal and regulatory requirements. Only four of the SOCs had electronic risk management information systems that were fully utilised and functional, and that formed the core of their risk management planning and decision-making. The remaining SOCs had devised measures to acquire the appropriate technology as part of their improvement commitments.

Processes to ensure governance of risk by the boards of directors and by operational committees are detailed in Table 4. These were the main themes that emerged from the document analysis at all seven SOCs.

TABLE 4: ERM governance: main responsibilities of the board and operational committees

Boards of Directors (either audit or risk, or combined)	Operational committees (either corporate or divisional)
1. Reviewing reports detailing the adequacy and effectiveness of the SOC's risk management function	1. Developing and ensuring compliance with philosophy, strategies, policies, frameworks, and procedures regarding risk
2. Assessing significant risk control failings or weaknesses and their potential impact. Confirming that appropriate action has been or is being taken	2. Reviewing the adequacy and overall effectiveness of the SOC's risk management and its implementation by management
3. Reviewing the ERM framework, risk philosophy, strategies, policies, and processes	3. Determining the structures and systems to be used by the SOC to manage risks effectively
4. Reviewing the acceptability of the SOC risk profile with reference to the overall risk appetite of the SOC by taking into account all risk-mitigation factors	4. Reporting to executive management committees and board sub-committees and, where required, to the board
5. Ensuring compliance with SOC risk policies and strategy, and with the overall risk profile of the SOC.	5. Reviewing the internal audit plan to ensure alignment with ERM registers i.e. ensuring that the audit plan is risk-based

Source: Derived from document analysis

Various ERM focus areas were also identified from the analysis of the ERM-related documents. These focus areas are noted in Table 5.

TABLE 5: ERM focus areas

ERM focus areas	Analysis
1. Business continuity	Three of the SOCs had undertaken business impact analyses of their critical business operations. In addition, business continuity plans had been devised, and progress was being monitored on a quarterly basis

management (BCM)	by the SOCs. The remaining four SOCs were in the process of devising their BCM frameworks, which would be followed by business impact analyses of their critical business operations
2. Fraud prevention	All the SOCs had developed fraud prevention plans, with implementation being monitored quarterly. However, only four of the seven of the SOCs had undertaken a fraud risk assessment to identify vulnerable business areas. The remaining three SOCs had plans to undertake a similar assessment within the next financial year
3. Legal and regulatory compliance	Four of the SOCs had a dedicated compliance function that was tasked with overseeing and ensuring both legislative and regulatory compliance throughout the SOC. The remaining three SOCs had commenced with a compliance assessment process and were working towards a fully integrated compliance management system
4. Risk finance (insurance aspects)	All SOCs had adequate insurance measures in place to respond to loss events. Two of the SOCs had established their own insurance companies to cater to their unique insurance needs; these had been in operation for many years
5. Risk-based internal audit	At all of the SOCs, the internal audit function did not reside within the SOC ERM portfolio. Internal audit plans of all SOCs were aligned with their ERM risk registers to ensure a link between their internal audit functions and ERM processes

Source: Derived from document analysis

These ERM operational areas included business continuity management, fraud prevention, legal and regulatory compliance, risk finance (insurance portfolio management), and risk-based internal auditing. These areas exposed the businesses to risks that had high levels of certainty of occurring.

In summary, from the document review, the following suggested practices in ERM emerged: acceptance of internationally recognised frameworks and methodologies to guide ERM strategies; the institution of governance structures involving the boards of directors and operational committees; and the identification of specific ERM focus areas, or processes that covered the management of business continuity, the prevention of fraud, compliance to laws

and regulations, financial coverage of risk and the undertaking of internal audits that were based on risk management.

6.2 Phase 2: Delphi survey

In Table 6, the ERM components identified in Round 1 are presented along with the frequency of the selection of each component by the participants.

TABLE 6: ERM components identified in Round 1

ERM component	Frequency
ERM governance structures	14
ERM oversight structures	14
Effectiveness of the board with regard to ERM	14
Organisational ERM structures	14
ERM culture	14
Accountability and responsibilities for ERM	14
Leadership approach	14
ERM policy and framework	12
ERM processes	12
ERM software utilisation	12

ERM component	Frequency
ERM integration with key organisational business processes	10
Level of experience of ERM staff	8
ERM capabilities across the organisation	8
ERM monitoring and review	8
ERM maturity and improvement opportunities	8
ERM reporting requirements to all stakeholders	8
Required ERM disclosures	8
Identification and reporting of emergent risks	7
External event or market influences	7
Integrity and accuracy of risk registers across SOCs	3
Status of risk registers	3
Application of the concepts of risk tolerance and appetite	3

Source: Derived from Delphi survey

Some identified ERM components shared common elements and so were consolidated. As a result, five main ERM themes were identified. These findings and the relevant areas that would need to be assessed relating to each theme are noted in Table 7.

TABLE 7: ERM themes and related assessment areas

ERM theme	Assessment areas
ERM organisational culture	Governance structures, ERM training, communication, leadership, ERM policy, stakeholder relations
ERM processes	ERM methodology (quantitative and qualitative), risk tolerance and appetite levels, risk analyses, risk assessment process, ERM reporting
ERM integration with business practices	Linkage between internal auditing, strategy processes, balanced performance frameworks, and management processes
ERM monitoring and controls	Emergent risks, reputation, and business continuity management
Asset and liability management	Budget variations, fraud, market and credit risk, funding, liquidity

Source: Derived from Delphi survey

In Round 2 of the Delphi process, the participants were requested to indicate their agreement or disagreement with the developed ERM themes, indicate whether any additional themes should be considered, and rate the ERM themes in terms of importance, to arrive at a total of 100% as noted in Table 8.

TABLE 8: Round 2 prioritisation of themes

ERM theme	Average level of importance (%)
ERM organisational culture	27
ERM processes	25
ERM integration with other business processes	19
ERM monitoring and controls	19

ERM theme	Average level of importance (%)
ERM asset and liability management	10
Total	100

Source: Derived from Delphi survey

All participants in Round 2 agreed with the ERM themes and no further additions were proposed.

During Round 3 of the Delphi, the Round 2 results pertaining to the ERM themes and their assigned average levels of importance were presented to the participants who were then requested to consider and comment on these results. All participants were in agreement with the results and, therefore, no further additions were made. The Delphi process was concluded.

Table 9 presents the consolidation of the ERM themes collated from the SOC document analysis and the Delphi process.

TABLE 9: Consolidated ERM themes

ERM themes	Components
ERM organisational culture/governance	Institution of governance structures (including involvement of boards of directors and operational committees); provision of ERM training; communication with stakeholders; leadership; ERM policy development; stakeholder relations
ERM processes	Adoption of ERM methodology (quantitative and qualitative); articulation of risk tolerance and risk appetite levels; undertaking of risk analyses; development of risk assessment processes; ERM reporting
ERM integration with other business	Establishing linkages between internal auditing, strategy

ERM themes	Components
processes	processes, balanced performance frameworks, and management processes; ensuring business continuity
ERM monitoring and controls	Monitoring of emergent risks including reputational risk; business continuity management; compliance with laws and regulations; internal risk-based auditing
ERM asset and liability management	Identification of budget variations, fraud, market and credit risk, funding, liquidity

Source: Derived from the document analysis and the Delphi survey

7. DISCUSSION

In summary, from the document review, it can be seen that measures had been adopted, to varying degrees, at all SOCs to address risk with boards of directors tasked with providing an oversight role. Common themes that emerged from the document review and the Delphi for consideration by SOC leaders were: ERM organisational culture (including governance), ERM processes, ERM integration with other business strategies, ERM monitoring and controls, and ERM asset and liability management. It is proposed that these components of risk management should be considered at South African SOCs.

The above themes were raised in the literature. The importance of governance, in general (Shank *et al.* 2013:385), and for SOCs in particular (OECD 2015:8), has been highlighted. Various theorists have noted the importance of embedding ERM into the culture of organisations (cf. O'Donnell 2005:180) as well as have stressed the importance of the commitment of leadership to any risk management process (cf. Coetzee & Lubbe 2013:51). Lindqvist (2014:394) discusses the central role in ERM of organisational control measures, communication, risk management and risk assessment in ERM. Adhering to a sound ERM methodology and framework has also been advocated (COSO 2004:3).

The sound governance of organisations, including SOCs, has increasingly commanded business attention (Balgobin 2008:18). Within the ambit of governance, risk management is

of central importance (Lundqvist 2014:393), demanding that issues such as organisational culture (O'Donnel 2005:178), leadership (Coetzee & Lubbe 2013:51), as well as processes and monitoring mechanisms (COSO 2004:75) are supportive of risk management strategies. The risk level SOCs should strive to attain is that of managed risk (Risk Management Development Program Collaboration 2002:15) where risk awareness is embedded in the organisational culture and where risks are proactively managed.

Qualitative studies run the danger of subjectivity that could exist in the interpretation of findings. Such subjectivity could occur in the interpretation of documentation and in the grouping of Delphi responses. The SOCs involved in the study comprised only the large Schedule 2 SOCs (Republic of South Africa 2015:22).

Accordingly, the recommendations should be generalised to all SOCs with caution. In addition, the involvement in the Delphi survey of some experts who were also employed at some of the seven SOCs could have resulted in bias in responses. Accordingly, this limitation must be born in mind in the interpretation of the findings.

Future studies should be undertaken across a wider sample of SOCs in South Africa, due to the important role played by SOCs in financial, investment, labour, technology, and infrastructure resources across sub-Saharan Africa. It is important that all SOCs assess their ERM processes to minimise or eliminate risk exposures that have a negative impact on organisational performance (Beasley *et al.* 2005:530; Buehler *et al.* 2008:106; O'Donnell 2005:177). This would enable SOCs to better manage the overall risk exposure as recommended by the King Reports on corporate governance (IOD 2002:73; 2009:14) as well as the ISO 31000 Risk Management Standard (ISO 2009:9), and the COSO ERM framework (COSO 2004:3).

Future studies should also investigate business sector-specific ERM process benchmarks within the SOC sector. These benchmarks could ensure the implementation of effective ERM processes that can be maintained and measured across all business sectors. Furthermore, such benchmarks would allow SOCs to compare the performance of their ERM processes against each other.

8. CONTRIBUTION OF THE RESEARCH

The objective of the study was to identify those components of risk that should be incorporated into ERM at South African SOCs. The implication of the study for SOCs is that leaders of these organisations may be better positioned to incorporate ERM as an integral part of their strategic and operational processes. Such integration would allow SOCs to refine their current ERM processes in order to explore the potential opportunities that are presented by risk exposure. In this regard, the identified ERM themes could serve as a checklist at SOCs to ensure that the major ERM areas are adequately identified and strategies devised to proactively address risk exposure in these areas. The aim of the adoption of an holistic ERM process is to ensure that SOCs move towards the managed tier of risk (Risk Management Research and Development Program Collaboration 2002:14).

9. CONCLUSION

SOCs have an economic function that cannot be successfully fulfilled by private companies or government departments. This function is one of critical importance to the well-being of all citizens, and to the competitiveness of private sector companies and industries in a developing country such as South Africa (OECD 2005:8).

Given that the public sector lags behind the private sector in risk management (AD-SA 2014:70; Coetzee & Lubbe 2013:50), along with the central role they play in advancing the well-being of citizens (Republic of South Africa 2011:67), it is critical that this aspect of governance is addressed. In this regard, the leaders of SOCs are encouraged to embark on holistic ERM that enables systematic risk assessment and management across all functions of the business.

REFERENCES

AEBI V, SABATO G & SCHMID M. 2012. Risk management, corporate governance, and bank performance in the financial crisis. *Journal of Banking & Finance* 36:3213-3226.

AG-SA see **AUDITOR GENERAL SOUTH AFRICA**.

AUDITOR GENERAL SOUTH AFRICA. 2011. Consolidated Provincial PFMA audit outcomes 2009-10. Pretoria: Auditor General South Africa.

AUDITOR GENERAL SOUTH AFRICA. 2013. Consolidated Provincial PFMA audit outcomes 2012-13. Pretoria: Auditor General South Africa.

AUDITOR GENERAL SOUTH AFRICA. 2014. Consolidated Provincial PFMA audit outcomes 2013-14. Pretoria: Auditor General South Africa.

BALGOBIN RNS. 2008. Global governance practice: the impact of measures taken to restore trust in corporate governance practice internationally. *The ICFAI Journal of Corporate Governance* VII(1):7-21.

BAXTER R, BEDARD JC, HOITASH R & YEZEGEL A. 2013. Enterprise Risk Management program quality: determinants, value relevance, and the financial crisis. *Contemporary Accounting Research* 30(4):1264-1295.

BEASLEY MS, CLUNE R & HERMANSON DR. 2005. Enterprise risk management: an empirical analysis of factors associated with the extent of implementation. *Journal of Accounting and Public Policy* 24:521-531.

BROMILEY P, MCSHANE M, NAIR, A & RUSTAMBEKOV E. 2015. Enterprise Risk Management: review, critique, and research directions. *Long Range Planning* 48:2265-276.

BUEHLER K, FREEMAN A & HULME R. 2008. Owning the right risks. *Harvard Business Review* September:102-110.

CADBURY A. 2000. The corporate governance agenda. *Corporate Governance: An International Review* 8(1):7-15.

COETZEE GP & LUBBE D. 2013. The risk maturity of South African private and public sector organisations. *Southern African Journal of Accountability and Auditing Research* 14:45-56.

COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION. 2004. Enterprise Risk Management: integrated framework. Jersey City, NJ: COSO.

CORBETTA P. 2003. Social research: theory, methods and techniques. London, UK: Sage.

COSO see **COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION**

DELBECQ AL, VAN DE VEN AH & GUSTAFSON DH. 1975. Group techniques for program planning: a guide to nominal and Delphi processes. Glenview, IL: Scott & Foresman.

DEL BEL BELLUZ D. 2002. Modern risk management. *CA Magazine* 135(9):39-41.

DREW SAW & KENDRICK T. 2005. Risk management: the five pillars of corporate governance. *Journal of General Management* 31(2):19-36.

ERNST & YOUNG. 2006. Companies on risk: the benefits of alignment. London, UK: EYGM. (Survey No. DK 0004).

FLICK U. 2009. An introduction to qualitative research. 4th ed. London, UK: Sage.

FONE M & YOUNG PC. 2000. Public sector risk management. London, UK: Butterworth-Heinemann.

HEILIGTAG S, SCHLOSSER A & STEGMANN U. 2014. Enterprise-Risk-Management practices: where's the evidence? A survey across two European industries. McKinsey Working Papers on Risk. New York, NY: McKinsey & Company.

HILB M. 2005. New corporate governance: from good guidelines to great practice. *Corporate Governance: An International Review* 13(5):569-581.

HILLSON DA. 1997. Towards a risk maturity model. *The International Journal of Project & Business Risk Management* 1(1):35-45.

INSTITUTE OF DIRECTORS IN SOUTHERN AFRICA. 2002. The King code of corporate practices and conduct. Johannesburg: IOD.

INSTITUTE OF DIRECTORS IN SOUTHERN AFRICA. 2009. The King code of corporate practices and conduct. Johannesburg: IOD.

INSTITUTE OF RISK MANAGEMENT SOUTH AFRICA. 2004. IRMSA code of practice. Johannesburg: IRMSA.

INTERNATIONAL STANDARDS ORGANISATION. 2009. ISO 31000:2009 risk management: principles and guidelines. Geneva, CH: International Standards Organisation.

IOD see **INSTITUTE OF DIRECTORS**

IRMSA see **INSTITUTE OF RISK MANAGEMENT SOUTH AFRICA**

ISO see **INTERNATIONAL STANDARDS ORGANISATION**

KIMBROUGH RL & COMPONATION PJ. 2009. The relationship between organizational culture and enterprise risk management. *Engineering Management Journal* 21(2):18-26.

KLEFFNER AE, LEE RB & MCGANNON B. 2003. Stronger corporate governance and its implications on risk management: evidence from Canada. *Risk Management and Insurance Review* 6(1):53-73.

LAI FW, AZIZAN NA & SAMAD FA. 2010. A theoretical appraisal of value maximizing Enterprise Risk Management. *International Journal of Accounting Information Science and Leadership* 3(6):23-43.

LAM J. 2014. What is ERM? In Lam J (ed). Enterprise Risk Management: from incentives to controls. 2nd ed. New York, NY: Wiley. pp. 51-66.

LEITCH M. 2010. ISO 31000:2009 – the new international standard on risk management. *Risk Analysis* 30(6):887-892.

LINSTONE HA & TUROFF M. 1975. The Delphi method: techniques and applications. London, UK: Addison-Wesley.

LUNDQVIST SA. 2014. An exploratory study of Enterprise Risk Management: pillars of ERM. *Journal of Accounting, Auditing & Finance* 29(3):393-429.

LUNDQVIST SA. 2015. Why firms implement risk governance: stepping beyond traditional risk management to enterprise risk management. *Journal of Accounting and Public Policy* 34(5):441-466.

MANDE V, PARK YK & SON M. 2012. Equity or debt financing: does good corporate governance matter? *Corporate Governance: An International Review* 20(2):195-211.

MCCULLOCH G. 2004. Documentary research in education, history and the social sciences. New York, NY: Routledge.

MERRIAM SB. 2002. Qualitative research in practice: examples for discussion and analysis. New York, NY: Wiley.

MONKS RAG & MINOW N. 2004. Corporate governance. 3rd ed. Malden, MA: Blackwell.

O'DONNELL E. 2005. Enterprise Risk Management: a system-thinking framework for the event identification phase. *International Journal of Accounting Information Systems* 6(3):177-195.

OECD see **ORGANISATION FOR ECONOMIC AND CO-OPERATION DEVELOPMENT**

OLIVA FL. 2016. A maturity model for enterprise risk management. *International Journal of Production Economics* 173:66-79.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. 2005. OECD guidelines on corporate governance of state-owned enterprises. Paris, FR: OECD Publishing. (Guideline No. ISBN 92-64-00942-6).

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. 2009. The corporate governance lessons from the financial crises. Paris, FR: OECD Publishing.

PIPER A. 2014. New risks for public sector auditors. *Internal Auditor* April:52-57.

POWELL C. 2002. The Delphi technique: myths and realities. *Methodological Issues in Nursing Research* 41(3):376-382.

PRIOR L. 2003. Using documents in social research. Thousand Oaks, CA: Sage.

RAPLEY T. 2007. Doing conversation, discourse and document analysis. London, UK: Sage. (book 7 of the SAGE qualitative research kit).

REPUBLIC OF SOUTH AFRICA. 1999. Public Finance Management Act No. 1 of 1999. Pretoria: Government Printer. (Government Gazette 33059).

REPUBLIC OF SOUTH AFRICA. 2010. National treasury report on public institutions listed in PFMA schedule 1, 2, 3A, 3B, 3C and 3D. Pretoria: Government Printer.

REPUBLIC OF SOUTH AFRICA. 2011. Presidential review committee on State-Owned Enterprises. Pretoria: Government Printer.

REPUBLIC OF SOUTH AFRICA. 2015. Annual performance plan 2015/16: Department of Public Enterprises. Pretoria: Government Printer.

RISK MANAGEMENT RESEARCH AND DEVELOPMENT PROGRAM COLLABORATION. 2002. Risk management maturity level development. San Diego, CA: International Council of Systems Engineering Risk Management Working Group.

SHANK T, HILL RP & STANG J. 2013. Do investors benefit from good corporate governance? *Corporate Governance: The International Journal of Business in Society* 13(4):384-396.

SOUTH AFRICAN GOVERNMENT COMMUNICATION AND INFORMATION SYSTEM. 2015. Minister Lynne Brown: Public Enterprise department budget vote 2015/16. Pretoria: Government Printers.

STANDARDS AUSTRALIA AND STANDARDS NEW ZEALAND. 2004. Australian/New Zealand standard 4360:2004: risk management. Sydney and Wellington: Standards Australia and Standards New Zealand.

STROH PJ. 2005. Enterprise risk management at United Health Group. *Strategic Finance* July:27-35.

VAN WYK J, DAHMER W & CUSTY MC. 2004. Risk management and the business environment in South Africa. *Long Range Planning* 37(3):259-276.

YARAGHI N & LANGHE RG. 2011. Critical success factors for risk management systems. *Journal of Risk Research* 14(5):551-581.