DETERMINANTS FOR A RISK-BASED AUDIT OF AN OPERATIONAL RISK MANAGEMENT FRAMEWORK: A SOUTH AFRICAN PERSPECTIVE

Young, Jacobus, University of South Africa

ABSTRACT

Many organisations are suffering losses due to ineffective risk management and audit functions. Based on the principles of the three lines of defence, it is clear that the functions of risk management and internal audit should be separated. The concept of a risk-based audit is currently evolving in such a way to ensure that organisations experience the maximum benefits of each function in a mutually exclusive way. A literature review was used to identify criteria to clarify the roles and responsibilities of each function and to serve as a platform to identify determinants for a risk-based audit approach of an operational risk management framework, which emphasises the primary role of internal audit, namely to provide management with the assurance that risks are being managed according to approved policies and procedures. Descriptive analysis of the response of a survey confirmed the importance of the determinants and indicated the current applicability thereof in various organisations.

Keywords: Risk Lines of Defense, Risk-Based Audit, Risk Management, Operational Risk Management Framework, Risk Governance, Risk Culture, Risk Management Process, Risk Identification, Risk Assessment, Risk Controls, Risk Monitoring, Risk Management Strategy, Risk Structure, Risk Governance.

INTRODUCTION

During the past two decades, operational risk management developed into an important management discipline for public and private organisations. In the early stages of implementing risk management, it was placed in the same department as internal audit. However, according to Swenson (2003), organisations were encouraged to establish independent internal audit and risk management functions in their structural hierarchies. This situation soon proved that the functions of operational risk management and internal audit should be separated in order to ensure the exploitation of the benefits of each function. Haubenstock (2003) stated that as operational risk management processes became more explicit, the role of internal audit also changed from assessing controls, to a modern approach on evaluating how well the overall risk management framework is functioning and the testing of controls. However, it is important that audit remains active in the risk management process and participating in assessments of the risk management framework to determine how well it has been developed and implemented across the businesses. Therefore, it became apparent that it is crucial that an organisation should have separate risk management and internal audit departments, although the detailed roles and responsibilities in terms of risk management are not always clear. This uncertainty between risk management and auditing could lead to serious risk incidents, which could have been prevented by instituting these functions as part of the risk governance of the organisation. Various disastrous incidents lead to a realization of the importance of risk management and internal audit as separate management functions.

From a South African perspective, the case of the collapse of African Bank is an example of a shortcoming of the risk management and audit functions. During the investigation, the Myburgh Commission determined that some of the reasons can be linked to operational risk factors reported by the City Press (2016) who stated that the "*directors were collectively in breach of their fiduciary and other duties to the bank.*" According to an investigation, the Chief Executive who "fought with his auditors and co-directors on how to report risk and impairments on bad loans…" can also be directly linked to a problem with governance and reporting, which are core factors of operational risk management that internal audit could have identified and reported to top management.

The recent incident concerning the VBS Mutual Bank (currently under investigation) that failed in March 2018 shows early signs of shortcomings of risk management. An investigation indicated that the Chairman and "four others" caused the collapse of the bank. They allegedly defrauded depositors by fabricating accounts, creating fictitious deposits, bribing officials, transferring funds to themselves and buying bank assets that were not recorded (Mkokeli & Bonorchis, 2018). A loss of approximately R1.9 billion that was looted caused the collapse of the VBS Mutual Bank and according to a report "there is no prospect of saving VBS." (Henderson & Bonorchis, 2018). It seems clear that fraudulent activities are the centre of this incident, which is another indicator that an effective operational risk management process could have proactively addressed. Unfortunately, this case also involves certain local municipalities who deposited funds with the VBS Mutual Bank and when requesting funds in February 2018, the Bank could not honor the requests and was subsequently placed under administration (Bonorchis, 2018). It seems that these municipalities decided to deposit their money with VBS without considering the potential consequences. In this case, it can be deduced that effective risk management and internal audit processes could have ensured sound risk-based decisions, preventing municipalities to deposit funds with the VBS Mutual Bank and avoided the alleged losses. Furthermore, an adequate internal audit function could proactively assess business decisions to determine if risk-taking and controls are in compliance with policy.

Another case is that of Steinhoff International Holdings, a major enterprise in the furniture and manufacturing field. According to Naude, Hamilton, Ungerer, Malan & de Klerk (2018), many questions were raised from a governance perspective and the role that shareholders played in failing to identify any problems regarding "accounting irregularities." After the announcement in December 2017, relating to these "accounting irregularities" the share price dropped catastrophically to R1.60 by May 2018. Although investigations are still in process, early concerns on the issue of efficiency of corporate governance, risk management and internal audit can be raised.

For effective operational risk management and internal audit functions, it is crucial to understand the roles and responsibilities of each function to ensure a risk-based approach to the management of risks by implementing a risk management framework. Therefore, the purpose of this article is to identify determinants for an operational risk management framework, which could also serve as a guide towards a risk-based audit approach. In this regard, the research question is: what are the determinants for a risk-based audit of an operational risk management framework and the current applicability of these determinants in organisations?

To answer this research question, this article deals with a literature review which can be used to derive the said determinants, that will be empirically tested to confirm its importance and to determine the current applicability in organisations.

The next section deals with the conceptual clarification of operational risk management

and internal audit, aiming to establish a clear understanding of each function, where-after a literature review on an operational risk management framework will be conducted.

CONCEPTUAL CLARIFICATION

In order to derive the determinants for a risk-based internal audit approach, a point of departure is to deal with the governance of operational risk in terms of the three lines of defence, followed by a review of the components of a typical operational risk management framework. There are many critics on the three lines of defence and some mentioned that the model is not perfect and perpetuates the idea that risk managers and internal auditors are there to prevent operating managers to take too much risk. However, Davies & Zhivitskaya (2016) state that in spite of the criticisms of the current three lines of defence model, it remains conceptually attractive and abandoning it without a well-articulated alternative would be a backward step. As such, the current model could serve as a platform to elaborate on the role and responsibilities of internal audit towards providing assurance that risks are being managed effectively. Although this article focuses on operational risk in terms of the three lines of defence, it can be expanded to involve other primary risk types such as market risk, credit risk and strategic risk.

Governance of Operational Risk

According to a Barnowl report on key changes in King IV (2016), the risk governance principle requires from governing bodies to govern risk in a way that supports the organisation in setting and achieving its strategic objectives. The governance of operational risk can be divided into three lines of defence, whereas the first line of defence is business management, the second line is risk management, and internal audit the third line.

First Line of Defence

According to the Basel Committee on Banking Supervision (BCBS) (2011), the first line of defence (business management) for operational risk means that the business owners are responsible for identifying and managing the risks inherent in the products, activities, processes and systems for which they are accountable. Blunden & Thirwell (2013) support this view by stating that the business lines are responsible and own the risks they generate. Mabwe, Ring & Webb (2017) inferred that the first line of defence consists of business frontline staff that undertake tasks within assigned limits of risk exposure and are responsible and accountable for identifying, assessing and controlling risks within their business functions. They are also responsible for implementing corrective actions to deal with control deficiencies. It is clear that the first line of defense is the actual risk owners and responsible for the daily risk management within the organisation. This view is supported by Chambers (2014) who stated that the first line of defence involves day-to-day risk management at operational levels.

Second Line of Defence

According to Girling (2013), the corporate operational risk function is the second line of defense, responsible for the operational risk framework and reporting on operational risk issues to top management. Mabwe et al. (2017) stated that the second line of defence concerns the designing of operational risk management tools to be used by the first line to identify and

manage risks and applies an independent challenge to the use of these tools. According to Bryce, Cheevers & Webb (2013), risk management monitors the risk policies, appetite and controls that the first line must follow.

Third Line of Defence

The third line of defence is internal audit and the importance of an independent and effective internal audit function as a core line of defence is emphasised by Bin Ibrahim (2016). According to Ernst & Young (2005), the internal audit function is one of the board's most powerful mechanisms for understanding the full spectrum of key risks facing the organisation and to monitor the effectiveness of related controls and risk management processes. According to the Chartered Institute of Internal Auditors (CIIA) (2017), the internal auditor will evaluate how well risks are being managed and will assess the quality of risk management processes, systems of internal controls and corporate governance processes across the organisation and report directly and independently to the most senior level of management. The important part of internal audit's function is the issue of providing an independent assurance to management that the first and second lines of defence are carrying out their functions effectively (McCormack & Sheen, 2013). According to Biljana & Blagica (2015), internal audit can use a risk assessment approach where all risks are evaluated and then play an advisory role in managing and reducing the risks for a smooth operation. It is essential that internal audit provides useful information and recommendations that will assist management in decision-making. For the purposes of this study, the following responsibilities of internal audit regarding risk management can be mentioned:

1. Evaluate and provide reasonable assurance that risk management, control and governance systems are functioning as intended and support the achievement of the organisation's objectives.
2. Assess risk exposures to protect the organisation by means of a risk-based independent assurance and recommended action plans.
3. Provide assurance to management on the design and working of the risk governance and the risk management process.
4. Provide assurance on the accuracy and reliability of the components of the risk assessment and reporting process (Blunden & Thirlwell, 2013).
5. Provide assurance regarding the processes of risk management (Biljana & Blagica, 2015).

In addition, the BCBS (2011) inferred that internal audit should be able to independently verify that the operational risk management framework has been implemented as intended and functioning effectively. It is clear that internal audit should include opining on the overall appropriateness and adequacy of the framework and the associated governance processes across the organisation. As such, audit should not simply be testing for compliance with board approved policies and procedures, but also be evaluating whether a framework meets organisational needs and supervisory expectations. Therefore, this research focuses on identifying the determinants derived from the components of a typical operational risk management framework. These determinants could assist internal audit with an approach to audit an operational risk management framework based on operational risk-related concepts.

It seems that the role of internal audit is changing from a reactive approach to a more proactive risk-based approach. The CIIA (2014) inferred that a risk-based audit approach is at the cutting edge of an internal audit practice and is evolving rapidly, while there is still little consensus about the best way to implement it. Risk-based internal auditing is defined as a methodology that links auditing to an organisation's risk management framework, which allows

internal audit to provide assurance to the board that risks are managed effectively in relation to the risk appetite (CIIA, 2014). In addition, Deloitte (2019) mentioned that the role of internal audit is evolving and the focus is shifting from providing assurance to a more advisory and anticipatory service to management. In this regard it seems important that internal audit also keep abreast with the ever- changing environment faced by operational risk managers. Operational risk management is continuously evolving and it is important that frameworks, policies, processes and systems be adapted with changing circumstances. This could be achieved by means of a risk-based audit and where management is willing to act promptly and appropriately on recommendations. Deloitte (2019) indicated, for example, that as cyber risk increases, internal audit needs to adapt and to move from IT and compliance-based approaches to a more risk-based approach.

The CIIA (2014) affirmed that the initial advantages of a risk-based internal audit can be summarised as follows:

1. Ensure that risks above and under the risk appetite threshold have been identified, assessed and responded to.
2. Ensure that the responses to risks are effective.
3. Ensure that where residual risks are not in line with the risk appetite, remedial action is taken.
4. Ensure that risk management processes including the effectiveness of responses and completion of actions are being monitored by management.
5. Ensure that risks and actions are being properly classified and reported.

It is evident that a risk-based audit approach could provide the board with assurance regarding the following:

1. Effectiveness of risk management processes.
2. Management of the risks classified as key risks, including the effectiveness of the controls.
3. Complete accurate and appropriate risk reports (CIIA, 2014).

It can be derived that internal audit must provide top management with an independent assurance that the organisation is managing its operational risks effectively and according to the approved policies, processes and systems. Furthermore, each line of defence plays a crucial role to ensure the effective management of operational risks of the organisation. According to Agarwal & Kallapur (2017), the objectives of the first line, second line and third line of defence are to implement risk management, risk oversight and assurance respectively. However, it is essential that all role players are knowledgeable with the roles and responsibilities of each line of defence to ensure the exploitation of each function to its fullest value to the organisation. From a risk management perspective, it is essential that internal audit provides assurance that an organisation's operational risk management framework is adequate and effective. Such an embedded framework will ensure a platform for effective risk management throughout the organisation.

Although it seems that the aforementioned roles and responsibilities are well-understood, a question that arises is: what determinants could internal audit use to ensure a risk-based audit approach for an operational risk management framework? To answer this question, it is necessary to briefly review the literature on operational risk management to be able to identify these determinants for a risk-based internal audit approach.

Operational Risk Management

Operational risk management is defined by the BCBS (2006) as a risk of loss due to inadequate or failed internal processes, people, systems or external events. This definition is accepted by most organisations. According to Chapman (2011), a risk management framework should assist an organisation in integrating risk management into its management processes to generate adequate risk information to serve as a platform for decision-making. The British International Standards Organisation (BS ISO) 31000 (2018) inferred that an embedded risk management framework should ensure that risk management forms an integral part of all activities throughout the organisation. According to Young (2018a), the components of a typical operational risk management framework are: a risk management culture; risk management strategy; risk management structures; and risk management process. Each of these components will be dealt with in more detail with the aim of identifying determinants for a risk-based audit of an operational risk management framework.

Risk Management Culture

According to the Committee of Sponsoring Organisations of the Treadway Commission (COSO) (2016), an organisation's culture reflects the ethics, values, beliefs, attitudes, desired behaviours and understanding of risk. As such, an operational risk management culture should also support the achievement of the organisation's vision, mission and strategic objectives. An important aspect of an operational risk management culture is to have an embedded definition for operational risk included in a board-approved operational risk management policy. Chapman (2011) stated that a risk policy should include the organisation's declaration of the importance of risk management in support of the realisation of its purpose, vision, strategic and business objectives. It should, furthermore, include a description of specific roles and responsibilities of the board, internal audit, governance committees, and employees. What is important is that the risk policy should describe the relationship between risk management, governance and internal audit. In addition, Girling (2013) mentioned that a risk policy should be approved by the board and according to the BCBS (2011), risk policies should be reviewed whenever a change in the operational risk profile occurs. According to Deloitte (2019), internal audit can help the board to drive the right culture and to assess it to provide advice to management regarding its framework for a risk culture. Based on the aforementioned, it is clear that an important determinant of an effective operational risk management framework is that a risk management culture should reflect the organisation's ethics, values and attitude towards operational risk management. The culture should be incorporated into an operational risk management policy and approved by the board.

Risk Management Strategy

A risk management strategy should ensure an integrated approach with the organisation's strategic process. According to COSO (2016), strategic objectives are high-level goals that are aligned with the organisation's mission, vision and strategic objectives. During the consideration of these strategic objectives, management should identify associated risks and its potential implications. According to the Association of Insurance and Risk Managers (AIRMIC) (2010), risk management should be a continuous process that supports the development and implementation of the organisation's strategy. During this process it is essential that the

organisation's risk appetite statement for operational risks is clearly defined. Girling (2013) stated that risk appetite is the amount of risk the organisation is willing to take and that the formulation thereof forms an integral part of an organisation's strategic planning process. It is clear that the setting of a realistic risk appetite for the organisation can be regarded as a primary objective of a strategic management process. However, it is important that the risk management process forms part of an integrated strategic planning process of an organisation. From an auditing perspective, the BCBS (2011) inferred that internal audit should not set the risk appetite or tolerance, but review the robustness of the process and how the limits are set and how they are adjusted to changing circumstances. Therefore, it is important for internal audit to utilise the existing risk methodologies to generate risk information in order to confirm the accuracy of the processes to set the risk appetite and tolerance levels.

The relevance of this section shows that a determinant of an operational risk management framework is that a strategic management process of the business should integrate a risk management process at a strategic level to identify the high-level operational risk exposures. Furthermore, the setting of a realistic risk appetite should be formulated and approved during the strategic business process and the role of internal audit should be to review the robustness of this process and to determine if the risk tolerance limits are realistic according to the strategic objectives. It is important that internal audit utilises the risk management methodologies to generate risk information during this process.

Risk Management Structure

A risk management structure should include the roles and responsibilities to govern the management of operational risks. According to Coetzee (2016), an organisation requires a unique risk management structure according to its needs, based on the business strategy. Such a structure should include all levels of management involved in risk management.

According to Young (2018b), there should be transparent, well-defined and consistent lines of responsibilities throughout the organisation to ensure an effective system of risk governance. Therefore, it is important that the roles and responsibilities of each level be clearly stipulated in order to prevent a duplication of tasks which could lead to confusion or neglecting risks that must be managed. According to the Institute of Operational Risk (IOR) (2010), all employees at all management levels should be clear as to their roles and responsibilities regarding risk management. It is furthermore, important that the audit and risk committees be properly mandated by the board to fulfill their roles regarding operational risk management.

The relevance of this section relates to the identifying of a determinant that relates to a risk management structure that specifies the roles and responsibilities of all role players according to the three lines of defence and that it is incorporated into a policy. Furthermore, the risk and audit committees should be clearly mandated by the board. Finally, it is imperative that all employees should be clear on their responsibilities regarding risk management.

Risk Management Process

A risk management process aims to identify, assess, mitigate and monitor the risks. The International Standards Organisation (ISO) 31000 (2009) inferred that a risk management process is one that systematically applies management policies, procedures and practices to identify, analyse, evaluate, treat, monitor and review risk. In support, Van Wyk, Bowen & Akintoye (2008) mentioned that a risk management process entails the identification, analysis,

mitigation, monitoring and reporting of risk. Methodologies that could be used in this regard are, for example: Loss Incident Database, Risk and Control Self-Assessments, Key Risk Indicators and Scenarios. Each component of an operational risk management process and the appropriate risk methodologies will be explained to serve as a platform to identify determinants to establish an operational risk management framework.

Risk Identification

According to the South African Local Government Association (SALGA) (2017), risk identification is a deliberate effort to identify and document an organisation's risk and is a rigorous and ongoing process that includes mechanisms to identify new and emerging risks timeously. Risk identification aims to identify the risk exposures that could possibly affect the achievement of business objectives of an organisation (ISO 31000, 2009). The risk identification starts with an analysis of the business processes, which entails an analysis of the business strategies and processes to identify the inherent risks (Young, 2016). According to Chapman (2011), risk identification is regarded as a process involving experienced staff that will generate a series of risks and opportunities, which could be included in a risk register. Apart from an analysis of the business processes, the organisation's loss history can also be used to identify risk exposures. According to Kalyvas & Akkizidiz (2006), management should ensure that operational risk loss event information is acquired throughout the organisation and included in a Loss Incident Database and eventually used to compile a risk register. In addition, an organisation can use scenarios to identify risks, which is regarded as a methodical way of getting professional opinions from business and risk managers to gain a rational evaluation of the probability and impact of potential operational losses (Kalyvas & Akkizidis, 2006). Girling (2013) confirmed that organisations use scenarios to evaluate their exposures to high-impact risk events. Scenarios can assist an organisation to understand its limits when setting a realistic risk appetite and could feed into capital and liquidity planning by providing useful information for financial planning (Blunden & Thirlwell, 2013). It is clear that a Loss Incident Database and Scenarios form an integral part of identifying inherent operational risks which should be included in a risk register. Once the risk register is completed, the next step is to assess the risks.

Risk Assessment

According to Ernst & Young (2005), the risks that matter the most organisations are the risks that have the greatest negative impact on value. Risk assessments tend to focus only on the process level and it is crucial that the key business risks are truly addressed through a confined process. According to Croitoru (2014), the aim of risk assessments is to perceive exposed processes carried out according to the likelihood of occurrences and the potential financial consequence for the organisation. According to ISO 31000 (2009), a risk assessment serves to assist in making decisions, based on the outcomes of risk analysis to determine which risks need to be prioritised and treated. Ernst & Young (2005) stated that risk assessments should be evolved into a consistent, embedded activity within an organisation's strategic, business, budget and audit planning processes, rather than executed as a significant stand-alone process. It can be concluded that a risk assessment entails the analysis of the identified risks to ascertain the potential likelihood and impact of the risks. This can be achieved by means of a Risk and Control Self- Assessment (RCSA) process. Such a process is based on events that happened in the past and uses current risk information to predict the future risk exposures, threats and

opportunities. According to King (2001), RCSAs are used to identify important risks to an organisation whereby responsible parties are requested to subjectively assess various parts of the organisation and its characteristics. Girling (2013) inferred that RCSAs are used to identify risks and assess it with the aim to control and mitigate the unacceptable risks. Chapman (2011) reasoned that risk evaluation aims to assess the identified risks as well as potential opportunities for the business. Blunden & Thirlwell (2013) added that RCSAs performed at an activity level will produce a significant number of risks and controls. From an internal audit perspective, Deloitte (2019) mentioned that continuous monitoring and assessments can assist auditors to direct its resources where most needed. This could assist audit to more effectively anticipate risks and advise management accordingly. It can be deduced that a RCSA process is a bottom-up activity that includes all employees involved in the business processes. It is essential that the assessed risks be included in a risk register and made available for decisions regarding control actions.

Risk Mitigation and Control

Olson & Wu (2008) mentioned that risk control relates to implementing control measures to minimise the effect or avoid the consequence of risk events. According to Croitoru (2014), risk control endeavours to convert uncertainties into an advantage for the organisation, restricting the level of risk exposure. Chapman (2011) stated that the risk control measures must be relevant in terms of significant issues or events and associated with the primary business objectives. It is clear that risk mitigation and control is a dynamic process, which requires the continuous updating of the risk register according to changing circumstances that could lead to new risk exposures. This highlights the importance of a continuous risk monitoring process.

Risk Monitoring

According to the ISO 31000 (2009), the monitoring of risks should be planned to ensure that the risk control and treatment measures are effective. Chapman (2011) inferred that the main goal of the monitoring of risks is to observe the functioning of risk control actions and to advise on the need for proactive management intervention. Deloitte (2019) mentioned that continuous risk assessments can lead to ongoing monitoring of risks across the organisation. While internal audit should not absorb management's risk identification responsibilities, they should have the tools to view and alert the organisation to emerging risks by means of continuous monitoring. The monitoring process will be sufficient when it has satisfied the following sub-objectives:

1. The development of warning indicators.
2. The monitoring of the internal and external context to ensure the determination of opportunities and risks.
3. The timeous implementing of responses to risks and opportunities.
4. The continuous updating of risk registers regarding changing circumstances and related actions.
5. The reporting on risk management actions to provide a view on the progress made in the success or failure of these actions.

According to Dowd (2003), the result of a risk identification and evaluation process is most likely a number of risk indicators, which could assist with the continuous monitoring of operational risks. Chapman (2011) inferred that risk indicators are used to facilitate regular

assessments and monitoring of risk exposures and mitigating responses. Girling (2013) stated that Key Risk Indicators (KRIs) predict that a risk is changing and requires proactive intervention. According to Blunden & Thirlwell (2013), trends in KRIs can be forward looking, based on actual current and past data. This is also useful when creating scenarios to identify risk exposures. These indicators should be reviewed on a periodic basis to serve as an early warning system to initiate proactive control or preventative measures for risk exposures. According to COSO (2016), KRIs should be reported to the levels of the organisation that are in the best position to manage the onset of a risk where necessary.

Cleary & Malleret (2006) mentioned that it is management's responsibility to ensure that there are procedures in place to: monitor the events that could result in a loss; provide early warning of changing circumstances that could result in an increase in risk; and ensure that these observations are communicated promptly to the correct management level to address by means of appropriate decisions. The results of a monitoring process should be a risk report to management for decision-making (ISO 31000, 2009). Risk reporting also forms a crucial part of risk monitoring.

Risk Reporting

Haubenstock (2003) reiterates that reporting is important and it communicates the overall level of risk and highlights key trends or exceptions that may require management's attention. Makiwane & Padia (2012) mentioned that risk management forms an essential part of corporate governance, specifically aimed to identify threats to the business in order to proactively take appropriate action to protect the organisation. In this instance, it is crucial that management receives accurate and timeous risk reports. Hain (2009) mentioned that sound risk management depends on the support of employees and their willingness to provide adequate and true information, which can be achieved by effective risk reporting. According to Ong (2007), risk reporting aims to inform management, trigger actions and allocate resources where appropriate. Dowd (2003) inferred that an organisation must implement a system of internal reporting of risk with the reporting adhering to the needs of the end user. According to Chapman (2011), risk reporting is a sub-goal of communication and reports must be prepared on a regular basis advising of changes to the risk exposure and the degree of success being realised by risk response activities. According to ISO 31000 (2009), it is important to ensure that information about risk is adequately reported and used as a basis for decision-making and accountability at all relevant organisational levels. It is clear that risk reporting plays a crucial role in risk management and it is essential to ensure the provision of adequate and accurate risk information for decision-making. As such, from an internal auditing perspective, it is important that operational risk reporting should be evaluated in terms of accurate risk–related contents and submitted to the correct management level timeously. Therefore, it can be derived that the operational risk reports are important for a risk-based audit whereby internal audit could provide management with the assurance that the risk reports are effective, accurate in contents, timeous and initiate corrective actions where required.

The relevance of this section dealing with an operational risk management process is to identify potential determinants which can be used for a risk-based audit of an operational risk management framework. These determinants are listed from 11 to 22 in the ensuing section.

The deduced determinants for the purposes of this article were subjected to an empirical analysis to confirm its importance and level of current applicability which served as a platform for recommendations.

RESEARCH METHODOLOGY AND RESULTS

A list of twenty-two determinants was identified to ensure the implementation of an operational risk management framework. Although the list is non-exhaustive, the identified determinants aim to address each component of an operational risk management framework.

The determinants were subsequently subjected to a survey by means of a questionnaire. Respondents of various public and private organisations in South Africa were approached to participate in the survey, which aimed to firstly, determine their views on the importance of the determinants of an operational risk management framework and, secondly, to indicate the current applicability of the determinants within their organisations. The questionnaire was distributed to 50 practitioners in the field of risk management, internal audit and financial management. Based on a 5-point Likert scale, the response rate of 44% included representatives from focus areas of internal audit (30%), risk management (45%) and financial management (25%). Thirty-one percent of the respondents indicated that they have more than 10 years' experience and 25% between 5 to 10 years' experience in their current organisations. The response also indicated that 63% of the respondents have more than 10 years' experience in risk management. As such, it can be deduced that the respondents have a high level of experience in their current organisations and potential exposure to risk management, leading to an assumption that the response can be used to derive acceptable conclusions and recommendations.

The primary data was subjected to descriptive statistics according to the Data Analysis with Microsoft EXCEL, using the mean and standard deviation functions (Berk & Carey 2000). The collected and analysed data sets (Refer to Table 1) were used to confirm the conclusions regarding the importance of the determinants and its current applicability in terms of an operational risk management framework. These conclusions were then integrated with the assumptions and recommendations regarding the determining of the determinants for a risk-based audit of an operational risk management framework.

Table 1
ANALYSED DATA

Determinants	Average Rating of agree to a "degree" and to a "full degree"		Variance	Average rating		Standard Deviation	
	Importance	Applicability		Importance	Applicability	Importance	Applicability
1	93.3%	75.6%	17.8%	4.6	3.95	1.8771	1.3301
2	73.7%	84.1%	-10.4%	4.3	4.0	1.5811	1.5634
3	100%	82.2%	17.8%	4.45	4.0	1.0327	1.3944
4	96.3%	71.9%	24.4%	4.5	3.7	1.3451	1.2472
5	100%	80.4%	19.6%	3.35	3.9	1.3662	1.4142
6	93.3%	35.6%	57.8%	4.6	3.2	2.0354	1.2309
7	74.8%	54.8%	20%	4.5	3.35	1.9518	1.0929
8	93.3%	58.5%	34.8%	4.65	3.65	2.0354	0.8333
9	94.4%	76.3%	18.1%	4.55	4.05	2.5634	1.4813
10	89,6%	26.3%	63.3%	4.3	2.95	1.3093	1.7159
11	96.3%	63.3%	33%	4.85	3.65	2.0000	1.2472
12	82.2%	63.3%	18.9%	4.25	4.0	1.4813	0.7559
13	65.2%	46.7%	18.5%	3.9	3.3	1.3017	0.8333
14	96.3%	73.7%	22.6%	4.55	3.95	1.3451	1.2472
15	89.6%	59.6%	30%	4.1	3.5	2,1157	1.7728

16	59.6%	35.6%	24%	3.85	3.05	1.4907	1.7994
17	80.4%	38.1%	42.2%	4.05	3.35	1.3333	0.9428
18	96.3%	55.9%	40.4%	4.5	3.45	1.5735	1.5634
19	96.3%	43%	53.3%	4.6	3.55	2.2677	0.9718
20	67.4%	35.6%	31.9%	3.85	3.0	1.1547	1.1547
21	100%	54.1%	45.9%	4.5	3.7	1.6850	1.3706
22	88.9%	33.7%	55.2%	4.55	3.3	2.1666	1.1677

The determinants and the relevant conclusions, based on the data analysis, are summarised below according to the most appropriate component of an operational risk management framework.

Determinants for Risk Governance

Derived from the literature, three determinants for this component were identified, namely:

1. Determinant 1. Business managers are regarded as the risk owners (First line of defence).
2. Determinant 2. The risk management function is separated from the internal audit function (Second line of defence).
3. Determinant 3. Internal audit provides management with an independent assurance that operational risks are managed according to approved policies and processes (Third line of defence).

The response acknowledged the importance of the three lines of defence regarding risk management. Business managers are regarded as risk owners, while the independence between risk management and internal audit are also recognised. The crucial role of internal audit to provide an independent assurance to top management regarding the management of risks was specifically emphasised (Rating of 100%). The response to the current applicability of the determinants confirmed that most organisations recognise the different roles and responsibilities in terms of the three lines of defence (Rating of 82.2%). It is however, important that these roles and responsibilities be included in a risk management policy. These determinants should form part of a risk-based audit approach when auditing the governance of operational risk management as a component of an operational risk management framework. This will also provide management with the assurance that risk and internal audit are functioning in a mutually exclusive way.

Determinants for Risk Management Culture

An embedded risk management culture is an important part of an organisation's risk management to ensure the implementation of the underlying principles and that the benefits of managing risks are exploited to its fullest degree. The following determinants were identified:

1. Determinant 4. Internal audit utilises the risk management methodologies to generate risk information.
2. Determinant 5. A risk management culture reflects the organisation's ethics, values and attitude towards operational risk management, incorporated into an operational risk management policy and approved by the board.

The response confirmed the importance that internal audit should leverage on the results of the risk management methodologies for risk information (Rating 96.3%). An operational risk management policy as part of a risk management culture is also confirmed by a high rating of importance (100%). The current rating of applicability in organisations confirmed that internal audit does use the available risk methodologies for risk information (Rating of 71.9%). It

furthermore, indicated that most organisations do have an operational risk management policy in place (Rating of 80.4%). Due to the importance of these determinants, it is imperative that it forms part of a risk- based audit to provide management with the assurance of accurate risk information and that the risk policies and procedures are approved by the board and are appropriate and effective.

Determinants for Risk Management Strategy

Two determinants relating to a risk management strategy were derived:

1. Determinant 6. The strategic management process of the business entertains an integrated risk management process at strategic level to identify the high-level operational risk exposures. The response confirmed the importance of an integrated strategic and risk management process (93.3%), however the current applicability reflects a low rating (35.6%), leading to an assumption that organisations are not currently implementing an integrated risk management process at a strategic level. According to the literature, organisations should identify risks during the setting of strategic objectives, which can be achieved by means of an integrated strategic and risk management process. It seems that most organisations are not yet compliant with this determinant making it essential for a risk-based audit approach for an operational risk management framework.
2. Determinant 7. The operational risk appetite and tolerance levels are formulated and approved during the strategic business process. The role of internal audit should be to review the robustness of this process and to determine if the risk tolerance limits are realistic according to the strategic objectives. The response indicated an acceptable rating of importance (74.8%), but a relative low rating for current applicability (54.8%), indicating that the formulation of a risk appetite and tolerance levels could still be in a developing phase. Therefore, it is important that this determinant form part of a risk- based audit approach to provide assurance to management that the risk appetite and tolerance levels are determined and approved during the strategic management process.

Determinants for Risk Management Structure

According to the literature, a risk management structure is an essential component of an operational risk management framework. The derived determinants for this component are as follows:

1. Determinant 8. The roles and responsibilities for effective operational risk management are clearly defined and differentiated between business owners, risk management, internal audit and the board and included in an operational risk management policy. The response confirmed the importance of clear roles and responsibilities for operational risk management at all management levels and its inclusion in a risk policy. The response also indicated that most organisations recognise the importance (93.3%) of this determinant, although it seems that it still needs attention to adhere to a higher degree of implementation to ensure that roles and responsibilities are clearly formulated in a risk policy.
2. Determinant 9. The board risk committee is mandated by the board. This determinant is rated at a high importance level (94.4%), indicating that it is crucial that a board risk committee should be established and mandated by the board to ensure an adequate risk governance structure. The rating of the current applicability (76.3%) indicates that most organisations do have a risk management committee mandated by the board.
3. Determinant 10. The responsibility of risk management is incorporated into each employee's job description applicable to their level of employment. This determinant emphasises the participation of all employees in risk management and is rated at a high importance level (89.6%), however the current applicability rating is low (26.3%). Therefore, it can be assumed that this determinant still requires attention by most organisations to ensure the involvement of all employees in risk management.

Based on a relatively high average rating of importance of the above-mentioned

determinants (93.3%, 94.4% and 89.6% respectively), it can be concluded that they should be included in a risk- based audit approach.

Determinants for Risk Management Process

A risk management process is most probably the most important part of an operational risk management framework. The following identified determinants endeavours to cover the components of a typical risk management process as well as some of the methodologies.

1. Determinant 11. Risk identification is an integral part of a risk management process with the objective to identify operational risk exposures inherent to the business processes. Rated at a high average level of importance (96.3%) confirms risk identification as a crucial part of an operational risk management process. The current average applicability rating (63.3%) however does not reflect a current level of acceptability. Risk identification is a continuous process to identify risk exposures which could influence the business objectives and should form part of a risk-based audit approach to ensure that risks are proactively identified and controlled.
2. Determinant 12. Identified risks are included in a risk register. According to the response it is confirmed that a risk register forms an important part of a risk management process and the rating of the current applicability (82.2%), supports an assumption that the management of a risk register is an embedded process. It is however, an important determinant for a risk-based audit to assure that risk exposures are identified and recorded in a risk register.
3. Determinant 13. Scenarios form an integral part of a risk identification process to identify potential future operational risks which could influence business decisions. This determinant was rated at a relative low rating of importance (65.2%), which could be a result of a general lack of knowledge on the implementation thereof. A relative low rating for applicability (46.7%) supports an assumption that the use of scenarios to identify potential operational risks are still in a developing phase. In order to enhance the effectivity of an operational risk management framework, it seems essential to include this determinant in a risk-based audit approach.
4. Determinant 14. Risks are assessed to determine risk mitigation and control measures. The response confirms the significance of risk assessments to assist in making decisions in terms of risk mitigation and control measures (96.3%). The level of applicability indicated that this determinant is currently being implemented at an acceptable level (73.7%). It can be concluded that it should form part of a risk-based audit to provide management with the assurance that risks are assessed and that appropriate control measures are formulated.
5. Determinant 15. Risk and Control Self-Assessments evaluate the risks and identify business opportunities. The response indicated a relative high variance between importance and applicability (89.6% and 59.6% respectively) leading to an assumption that although Risk and Control Self-Assessments are being used, it can be expanded to add more value in terms of identifying business opportunities. Therefore, this determinant is essential for a risk-based audit to assure management that risks and business opportunities are assessed and identified respectively.
6. Determinant 16. A Risk and Control Self-Assessment is a bottom-up approach and involve all employees involved in the business process being assessed. Rated at a low importance (59.6%) and current applicability (35.6%) indicates that not all employees are involved in risk management, leaving a serious shortcoming in the effective management of risk exposures. Therefore, this determinant should be included in a risk- based audit approach to provide assurance that all employees are involved in risk management.
7. Determinant 17. Risk control measures are relevant and associated with the primary business objectives. A relative acceptable rate of importance (80.4%) and low rating of applicability (38.1%) of this determinant indicate that there could be an inadequacy in control measures in terms of the actual risks threatening the achievement of business objectives. Therefore, it is crucial that internal audit should assure, as part of a risk- based audit approach, that control measures are adequate.

8. Determinant 18. A risk monitoring process ensures that the risk control and treatment measures are effective. Rated at a high importance level (96.3%), confirms the significance of risk monitoring to observe the functioning of the risk control actions and to advise the need for proactive intervention. However, a relative low rating of the current applicability (55.9%) indicates that this determinant still requires attention. Therefore, it can be concluded that it should be included in a risk-based audit approach to provide assurance that the effectiveness of risk control measures is monitored.

9. Determinant 19. Risk monitoring ensures the timeous implementation of responses to risks and opportunities. A high importance rating (96.3%) confirms this determinant as a significant attribute to an effective operational risk management process. However, a low rating of current applicability (53.3%) indicates a scope for improvement, especially concerning the identifying of business opportunities. Risk monitoring should form part of a risk-based audit which could assure the timeous response to risks and identifying potential business opportunities.

10. Determinant 20. A Key Risk Indicator process is used for risk monitoring. Rated at a relative low importance rating (67.4%) and current applicability (35.6%) this determinant indicates that organisations are not using this risk methodology for risk monitoring to its fullest potential. Early warning is a crucial part of risk management, which can be established by means of managing KRIs. Therefore, it is important that this determinant be included in a risk-based audit approach to ensure that current risks are monitored and proactively addressed.

11. Determinant 21. There are clear reporting lines for operational risk reporting. A high importance rating (100%) confirms that operational risk reports are crucial for effective decision-making. A relative low rating of the current applicability (54.1%) leads to an assumption that the current reporting lines are not at an acceptable standard. The importance of this determinant confirms that it should be included in a risk-based audit to assure well-structured risk-reporting lines.

12. Determinant 22. Risk reporting is accurate, timeous and initiates effective risk decisions. The response emphasises the importance (88.9%) of risk reporting as an imperative component of an operational risk management process. The rating for applicability (33.7%), however, indicates that this determinant could be improved to ensure accurate risk reporting for decision-making. This determinant could also be regarded as an important attribute to a risk-based audit to provide management with the assurance that the risk reports are accurate and timeous for effective decision-making.

Based on the analysis indicating the variance between the level of importance and applicability, the top 5 determinants that require the most attention to reduce the gap are illustrated in Figure 1.

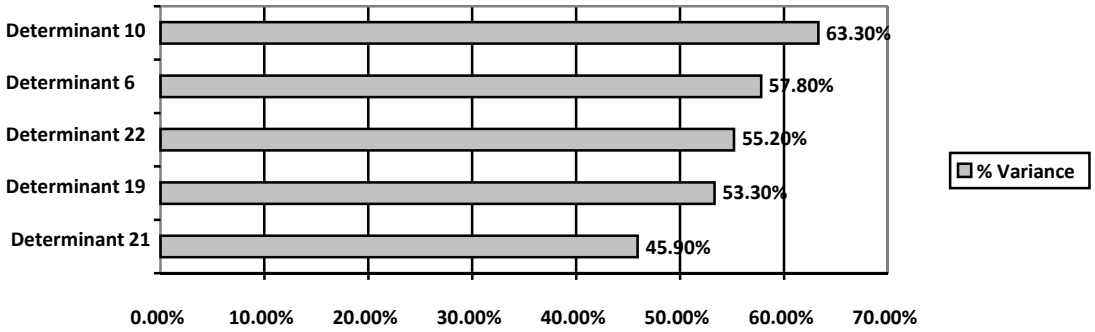

FIGURE 1
PERCENTAGE VARIANCE BETWEEN AVERAGE RATING OF IMPORTANCE AND APPLICABILITY

Determinant 10 shows the largest variance between the rating of importance and acceptability, which deals with the involvement of all employees in risk management. This is

followed by determinant 6 concerning an integrated strategic and risk management process and determinant 22 on accurate risk reporting. Determinants 19 and 21 deals with risk monitoring and risk reports for decision-making. The high variance for some of the determinants indicates that there is still room for improvement to increase its applicability to embed an effective operational risk management framework.

The next section deals with concluding remarks based on the literature and response on the importance and applicability of the determinants.

CONCLUSION

This study aimed to identify determinants which could serve as a guideline for a risk-based audit of an operational risk management framework. The main components of an operational risk management framework were identified as risk governance, risk culture, risk strategy, and a risk management process. A literature review was used to identify twenty-two determinants that were rated for importance and current applicability by means of a survey. Although some of the determinants were rated at a low current applicability, all determinants were rated as important to some degree to serve as a guideline for a risk-based audit approach.

An investigation of the African Bank saga, the collapse of the VBS Bank and the case of Steinhoff International Holdings revealed problems relating to governance, risk management and internal audit. It is envisaged that if the risk management and audit functions were effective and formed part of the risk governance processes, these events could have been prevented. For example, by adhering to the determinants the following could be achieved:

1. Adequate governance in terms of the appropriate allocation of roles and responsibilities for business management, risk management and internal audit regarding the management of risks.
2. Embedding of a risk culture, an integrated strategic management process, appropriate risk structures and an effective operational risk management process.
3. Providing management with the independent assurance that the risk management processes are adequate and executed according to approved policies.
4. Ensuring that management makes adequate risk-based decisions.

According to the identified gap between the importance and the current applicability of the determinants, it is clear that a risk-based approach to audit an operational risk management framework is imperative although it seems this concept is still at a grass root level. In addition, it is recommended that in general, special attention is given to enhance the following:

1. involving all employees in risk management;
2. integrating the strategic and risk management processes;
3. improving risk management reports for sound decision-making; and
4. improving risk monitoring to identify and respond to potential business opportunities.

The identified determinants are generic and applicable to all public and private organisations and can be used by internal audit as a guide towards a risk-based audit approach to provide independent assurance of an adequate operational risk management framework. The rated level of applicability of the determinants could also serve as a guideline for organisations to assess their own level of adherence to the determinants and to identify potential areas of development to ensure an adequate operational risk management framework. It is also envisaged

that the determinants could be expanded to include the auditing of other risk types such as credit risk, market risk and strategic risk in order to establish a holistic risk-based audit approach. Although certain roles and responsibilities of internal audit were determined in terms of a risk-based audit approach to provide management with the assurance of an effective operational risk management framework, further research could deal with more detail on the adequacy of the three lines of defence model relating to risk management.

REFERENCES

Agarwal, R., & Kallapur, S. (2017). Cognitive risk culture and advanced roles of actors in risk governance: A case study. *The Journal of Risk Finance, 19(4), 1-26.*

Association of Insurance and Risk Managers (AIRMIC). (2010). *A Structured Approach to Enterprise Risk Management and the Requirements of ISO 31000*. Published by The Association of Insurance and Risk Management (AIRMIC), The Public Sector Risk Management Association (ALARM) and the Institute of Risk Management (IRM): United Kingdom, 1-18.

BARNOWL (2016). Key changes in King IV. King IV Report: Risk, Compliance and Assurance. BARNOWL Insights, 9 December 2016. Retrieved from http://www.barnowl.co.za/insights/king-iv-report-risk-compliance-and-assurance/

Basel Committee on Banking Supervision. (2006). International Convergence of Capital Measurement and Capital Standards A Revised Framework Comprehensive Version. Bank for International Settlements, June 1-333. Retrieved August 21, 2019 from www.bis.org

Basel Committee on Banking Supervision. (2011). Principles for the Sound Management of Operational Risk Management. Bank for International Settlements, June 1-19. Retrieved from www.bis.org

Berk, K.N., & Carey, P.M. (2000). *Data Analysis with Microsoft EXCEL*. Brooks/Cole, a Division of Thompson Learning. Canada.

Biljana, A., & Blagica, K. (2015). The role of internal audit in risk management system of companies. *Economic Development.* Institute of Economic Development. UDC 657.6-051-057.3/:005.52.005.005.334(497.7). 3/2015 1- 10.

Bin Ibrahim, M. (2016). *Audit as a partner of change.* (Online) Government briefing: Governor of the Central Bank of Malaysia at the 5th PETRONAS Board Audit Committee Forum in Kuala Lumpur on 16 August 2016 1-4. Published by the Bank of International Settlements. Retrieved April 12, 2019 from https://www.bis.org

Blunden, T., & Thirlwell, J. (2013). *Mastering Operational Risk: A practical guide to understanding operational risk and how to manage it*. 2nd Edition. Pearson. Edinburgh.

Bonorchis, R. (2018). South Africa's VBS Mutual Bank Fails amid Severe Liquidity Crisis. *Bloomberg* (Online) March 1-3. Retrieved April 2, 2019 from https://.bloomberg.com/news/aricles/2018-03-11/s-africa-s-vbs-mutual- bank.fails-amid-sever-liquidity-crisis

British International Standards Organisation (2018) BISO 31000:2018: *Risk Management – Guidelines*. The British Standards Institution. Published by BSI Standards Limited. 2018 1-15.

Bryce, C., Cheevers, C. & Webb, R. (2013). Operational risk escalation: An empirical analysis of UK call centres. *International Review of Financial Analysis. Elserivier, 30*, 298-307.

Chambers, A. (2014). Maginot line, Potemkin village, Goodhart's law? Third line of defense: second thoughts (part 2). *Internal Auditing,* 29(1) 10-16. Thomas Reuters.

Chapman, R. (2011). *Simple tools and techniques for enterprise risk management*. 2nd Edition. John Wiley & Sons Ltd. West Sussex, England.

Chartered Institute of Internal Auditors. (2014). Risk-based internal auditing. Position paper dated 8 October 2014 1-3. Retrieved March 15, 2019 form www.iia.org.uk

Chartered Institute of Internal Auditors. (2017). What is Internal Audit? 24 August 2017 1-5. Retrieved March 15, 2019 from https://.iia.org.uk/about-us/what-us-internal-audit/

Cleary, S., & Malleret, T. (2006). *Resilience to Risk. Business success in turbulent times*. Human and Rousseau, A Division of NB Publishers (Pty) Ltd. Pretoria.

City Press. News24.com (2016). *Damning report strengthens the cases of those suing African Bank*. 14 May 2016. Retrieved from http://city-press.news24.com/Business/damning-report-strengthens-the-case-of-those-suing-african-bank-20160513

Coetzee, P. (2016). Contribution of internal auditing to risk management. Perceptions of public sector senior management. *International Journal of Public Sector Management.* 29(4) 348-364.

Committee of Sponsoring Organizations of the Treadway Commission. (2016). *Enterprise Risk Management. Aligning Risk with Strategy and Performance.* PriceWaterhouse Coopers. June 1-124. Retrieved from www.coso.org

Croitoru, I. (2014). Operational risk management and monitoring. *Journal: Internal Auditing and Risk Management.* 4(3) 21-31.

Davies, H., & Zhivitskaya, M. (2018). Three lines of defense: A robust organising framework, or just lines in the sand? *Journal: Global Policy,* 4(1), 34-42.

Deloitte (2019). Internal audit future trends and innovation. High-impact areas of focus: Internal audit trends 2019. Deloitte US 2019, 1-13. Retrieved from https://www2.deloitte.com/us/en/pages/risk/ artciles/internal- audit-future-trends.html

Dowd, V. (2003). Measurement of Operational Risk: the Basel approach, in Alexander C (Ed.), *Operational Risk. Regulation, Analysis and Management*. Pearson Education Ltd. Harlow.

Ernst & Young. (2005). Managing Risk across the Enterprise-Connecting New Challenges with Opportunities. A publication by Ernst & Young September 1-14. Retrieved 2018 from www.ey.com.

Girling, P. (2013). *Operational Risk Management. A complete guide to a successful operational risk framework.* John Wiley & Sons, Inc. New Jersey.

Hain, S. (2009). Managing Operational Risk: Incentives for reporting and disclosure. *Journal of Risk Management in Financial Institutions* 2(3) 284-300. Henry Stewart Publications.

Haubenstock, M. (2003). The operational risk management framework. In Alexander C (Ed), *Operational Risk. Regulation, Analysis and Management*. Pearson Education Ltd. Harlow.

Henderson, R., & Bonorchis, R. (2018). South African Probe Finds $130 Million Looted from Failed Bank. *Bloomberg* (Online). Retrieved from https://www.bloomberg.com/news/articles/2018-10-10/south-african-probe-finds-130-million-looted-from-failded-bank

Institute of Operational Risk. (2010). Operational risk sound practice guidance: Operational risk governance. Published by the Institute of Operational Risk. September 1-37. Retrieved from www.ior- institute.org

International Standards Organisation (2009) ISO 31000:2009: *Risk Management Principles and Guidelines*. International Organization for Standardization, Geneva, Switzerland. 2009 1-21. Retrieved from www.iso.org

Kalyvas, L., & Akkizidis, I. (2006). *Integrating Market, Credit and Operational Risk: A complete guide for bankers and risk professionals.* Published by Risk Books Incisive Financial Publishing Ltd. London.

King, J.L. (2001). *Operational Risk: Measurement and Modelling*. John Wiley & Sons, Inc. New Jersey, England.

Mabwe, K., Ring, P., & Webb, R. (2017). Operational risk and the three lines of defence in UK financial institutions: Is three really the magic number? *Journal of Operational Risk, 12*(1) 53-69. Risk Journals.

Makiwane, T., & Padia, N. (2012). Evaluation of corporate integrated reporting in South Africa post King III release South Africa: An exploratory enquiry. *Journal of Economic and Financial Sciences*, *6*(2) 421-438.

McCormack, P., & Sheen, A. (2013). Operational risk: Back on the agenda. *Journal of Risk Management in Financial Institutions*, *6*(4) 366-386.

Mkokeli, S., & Bonorchis, R. (2018). South Africa's biggest bank heist leaves trail of destruction. *Bloomberg*. Retrieved from https://www.bloomberg.com/news/articles/2018-07-30/- ponzi-scheme-at-small-south-african-bank-becomes-biggest-heist

Naude, P., Hamilton, B., Ungerer, M., Malan, D., & de Klerk, M. (2018). Business Perspectives of the Steinhoff Saga. *Special Report, Management Review*. Published by the University of Stellenbosch, June 2018.

Olson, D.L. & Wu, D.D. (2008). *Enterprise Risk Management*. World Scientific Publishing Co. Pty. Ltd. Singapore.

Ong, M. (2007). *The Basel Handbook. A guide for financial practitioners*. Published in Association with KPMG by Risk Books, a division of Incisive Financial Publishing Ltd. Haymarket.

South African Local Government Association. (2017). *Risk Management Framework*. 1-64. Pretoria. Retrieved from www.salga.org.za

Swenson, K. (2003). Measurement of Operational Risk: The Basel approach, in Alexander, C (Ed.), *Operational Risk. Regulation, Analysis and Management*. Pearson Education Ltd. Harlow.

Van Wyk, R., Bowen, P., & Akintoye, A. (2008). Project risk management practice: The case of a South African utility company. *International Journal of Project Management, (*26), 49-163.

Young, J. (2016). Risk management in corporate governance, in Botha, T. et al (Eds.), *Corporate Citizenship*. Oxford Press (Ed) in *Corporate Citizenship*. Published by Oxford University Press Southern Africa (Pty) Limited 133- 159.

Young, J. (2018a). *Operational Risk Management* (2nd revised edition). Van Schaik Publishers. Pretoria.
Young, J. (2018b). Guiding criteria for an operational risk management framework for South African Municipalities. *Administration Publication, 26*(1), 9-41.