



UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

Gordon Institute of Business Science

University of Pretoria

The impact of Enterprise Risk Management (ERM) on the internal control system of organisations in the mining industry

Thelma Kganakga

99162131

A research project submitted to the Gordon Institute of Business Science, University of Pretoria, in partial fulfilment of the requirements for the degree of Master of Business Administration.

11 November 2013

ABSTRACT

Economic markets continue to become more complex, creating challenges for organisations with the scope, complexity, and interdependencies of emerging risks necessitating a more robust and integrated approach to risk management and internal control. To this effect, enterprise risk management (ERM) has been the topic of increased attention with regulatory, business and academic arenas alluding to the need for ERM and improved internal control systems. The traditional practices of managing risks in silos has had implications on the internal control systems of organisations as the organisational focus has been on those directly related to financial operations and reporting.

Therefore, the aim of this study was to determine the extent to which organisations have implemented ERM, particularly those in the mining industry, and then understand the impact this ERM has on the internal control system. To this end, qualitative research with an exploratory design was conducted. Twelve executives and senior managers across eight organisations, who are responsible for risk management and assurance of internal controls, were interviewed to uncover their distinctive insights regarding this phenomena. The rich data that was unearthed was analysed using thematic analysis techniques.

The evidence from the study showed that while the ERM practices of organisations are between intermediate and mature levels, more work still needs to be done in order to institutionalise ERM. Furthermore, ERM improves the internal control system of the organisation, however the maturity of the ERM process and the leadership in the organisation are big determinants of the extent to which the improvements can be realised. Other factors were identified which necessitate enhancement and sustainability of the ERM capability and formed the basis of a model for enterprise risk and control integration that was developed. The results of this research provided additional insights that will bolster the advancement of internal control management through ERM.

Keywords: Enterprise risk management, internal control, mining industry, risk

DECLARATION

I declare that this research project is my own work. It is submitted in partial fulfilment of the requirements for the degree of Master of Business Administration at the Gordon Institute of Business Science, University of Pretoria. It has not been submitted before for any degree or examination in any other university. I further declare that I have obtained the necessary authorisation and consent to carry out this research.



Signed: Thelma Kganakga

11 November 2013

Date

ACKNOWLEDGEMENTS

I wish to express my thanks and appreciation to my Heavenly Father, God for giving me the strength and wisdom to complete this study. I am also grateful to my supervisor, Mr Ross Liston for his guidance and support throughout the study and for providing detailed comments to help solidify this material. My appreciation also goes to the respondents who participated in the study and gave so freely of their time. Without their willingness to participate, this research would not have been possible.

My deepest gratitude goes to my love Moses for walking this journey with me, providing valuable input to this research and pushing me do my best. To my friends, family, mentors, colleagues – thank you for your support throughout this journey and for giving me hope when the road looked dark. I am also grateful to my late grandmother, Mapitsoe Kganakga for always being my strength even in her absence, for she has always believed in my potential. I am very humbled by the love you have all given me.

To my fellow MBA class mates - *the Colombians*: this journey was fulfilling largely because of you. Thank you for making this journey a memorable experience in my life.

Thank you all!

TABLE OF CONTENTS

CHAPTER 1: INTRODUCTION TO RESEARCH PROBLEM	1
1.1 Introduction.....	1
1.2 Research Problem.....	1
1.3 Research Motivation.....	5
1.4 Research Objective	6
1.5 Scope of Research.....	7
1.6 Organisation of Research	7
CHAPTER 2: LITERATURE REVIEW	8
2.1 The Evolution of Enterprise Risk Management	8
2.2 Differentiating Traditional Risk Management and Enterprise Risk Management	10
2.3 Adoption of ERM as business imperative.....	13
2.3.1 ERM adoption in a complex industry driven by governance factors	15
2.4 Defining Internal Control and its role in the organisation	16
2.4.1 Significance of Risk Management in the Internal Control System	18
2.4.2 Challenges in the management of Internal Control	20
2.5 Responsibilities for ERM and Internal Control.....	20
2.6 Contingency and Institutional Theory interpretations of risk and control.....	22
2.6.1 Organisation size.....	23
2.6.2 Organisational Culture.....	23
2.6.3 Industry	24
2.7 Inferences drawn from the literature	25
2.8 Conclusion.....	26
CHAPTER 3: RESEARCH QUESTIONS	28
CHAPTER 4: RESEARCH METHODOLOGY	30
4.1 Research design and rationale	30
4.2 Population	31
4.3 Sampling method.....	32
4.3.1 Sampling technique and size.....	32
4.4 Unit of analysis	33
4.5 Method of data collection.....	33
4.5.1 Information gathering process	33
4.5.2 Research instrument	33
4.5.3 Cautions on potential bias arising from interviews	35

4.6	Pilot-testing.....	36
4.7	Data analysis approach	36
4.8	Validity and Reliability.....	38
4.9	Confidentiality and Anonymity.....	38
4.10	Research Limitations	39
CHAPTER 5: RESULTS		40
5.1	Introduction.....	40
5.2	Sample description and response rate.....	40
5.3	Research Question 1: To what extent have organisations adopted a formal enterprise-wide approach to risk management and why did they adopt it?.....	42
5.4	Research Question 2: How does ERM enhance an organisation’s internal control system?.....	50
5.5	Research Question 3: What are the key factors that are critical in ensuring that ERM enhances an organisation’s internal control system?	57
5.6	Other results presenting contextual considerations for ERM.....	61
5.7	Conclusion.....	63
CHAPTER 6: DISCUSSION OF RESULTS		64
6.1	Introduction.....	64
6.2	Research Question 1	64
6.2.1	Interpretation of results	64
6.2.2	Conclusion to research question 1	69
6.3	Research Question 2.....	69
6.3.1	Interpretation of results	69
6.3.2	Conclusion to research question 2.....	74
6.4	Research Question 3.....	74
6.4.1	Interpretation of results	75
6.4.2	Conclusion to research question 3.....	78
6.5	Conclusion.....	78
CHAPTER 7: CONCLUSION		80
7.1	Introduction.....	80
7.2	Review of research objectives	80
7.3	Major findings	80
7.4	Enhancing and sustaining the ERM capability	82
7.5	Recommendations for stakeholders.....	84
7.5.1	Recommendations for management and boards of directors	84
7.5.2	Recommendations for risk and internal audit practitioners.....	84

7.6	Recommendations for future research	85
7.7	Concluding remarks.....	86
REFERENCE LIST		87
APPENDIX 1: TYPICAL RISKS FACING MINING INDUSTRY		94
APPENDIX 2: LETTER OF CONSENT		96
APPENDIX 3: SEMI-STRUCTURED INTERVIEW GUIDE		97
APPENDIX 4: HIGH-LEVEL OVERVIEW OF TWO OF THE WIDELY USED ERM STANDARDS AND GUIDELINES.....		102

LIST OF FIGURES

Figure 1: Summary of the current scope and the extent of research.....	5
Figure 2: Evolution of Risk Management into Enterprise Risk Management.....	9
Figure 3: Typical descriptions of enterprise risk management maturity	14
Figure 4: Constructs Relationship diagram	26
Figure 5: Views on whether implementing ERM has enhanced the internal control system	57
Figure 6: A Model for Enterprise Risk and Control Integration	83
Figure 7: ISO 31000 Risk Management Guideline	102
Figure 8: COSO: 2004 Enterprise Risk Management Framework.....	103

LIST OF TABLES

Table 1: Key features of ERM versus traditional risk management	12
Table 2: Summary description of interviewees per company	41
Table 3: ERM Maturity of sample organisations	43
Table 4: Summary of contextual elements that influence ERM and internal control application	62
Table 5: Research question, emerging themes and summary themes	63
Table 6: The 12 most cited risks (in no particular order).....	94
Table 7: High-level overview of the ISO 31000 and COSO 2004	102

CHAPTER 1: INTRODUCTION TO RESEARCH PROBLEM

1.1 Introduction

Risk management has been a widely debated topic from the early days of finance research where according to McShane, Nair, and Rustambekov (2011) it was considered irrelevant under perfect market conditions. However, the changing economic and business landscape, for example supply chains, global trade, and financial markets all complexly linked, result in uncertainties in today's economy. Ionescu (2008) explains that every organisation is, to some extent, in the business of risk management, irrespective of what products or services the organisation delivers.

Organisations set strategic objectives for their businesses, and then manage risks that threaten the achievement of those objectives. Risk encompasses the uncertainty of future reward in terms of both the up-side (opportunities) and down-side (threats) (Vijayakumar & Nagaraja, 2012) Therefore, no organisation in any industry can do business without taking risk, especially in today's challenging global economy where business opportunities and risks are constantly changing, leading to significant impacts on company operations, reputations, and even survival.

1.2 Research Problem

The corporate scandals of the early 2000s which led to the collapse of companies such as Enron and WorldCom, and the recent global financial crisis have necessitated regulators to intensify their attention on risk management and internal controls. This has been reflected through the recent corporate governance guidelines and standards across the globe, emphasising the need for an enterprise-wide risk management and effective internal control management (Rae, Subramaniam, & Sands, 2008). These include guidelines and standards such as the Turnbull report in the United Kingdom, the Committee of Sponsoring Organisations (COSO) Enterprise Risk Management Integrated Framework, International Organisation for Standardization (ISO) 31000, the Sarbanes-Oxley Act of 2002 Section 404 and the South African King III report on Corporate Governance. As a result, organisations in the various sectors are faced with a growing number of options for managing the internal control system, including the adoption of enterprise risk management (ERM), ethical and board evaluation processes, risk and control self-assessments and a plethora of accounting-based controls (Cappelletti, 2009; Rae et al., 2008). Yet, there is little understanding on how

these various risk and control strategies and mechanisms affect each other (Rae et al., 2008). In an attempt to understand how these risk and control strategies affect each other, this study will focus on understanding how the adoption of ERM affects the internal control system of an organisation, particularly given that internal control management has been the focus of regulators and shareholders of organisations as far back as 1980's prior to the advent of ERM (Dickinson, 2001) The need for a better understanding of these relationships becomes even more crucial as the global survey report by PricewaterhouseCoopers (2012), showed that the majority of business leaders indicated that they were still not comfortable with how their risks were being managed, "despite the fact that 74% of those surveyed have formal enterprise risk management (ERM) processes in place" (p. 8).

In addition, a Risk and Insurance Management Society (2011) global survey on the extent of ERM adoption in organisations showed that 54% of companies have partially or fully implemented ERM Programs. The study was carried out among 1,431 risk managers from 11 different industries This number, according to the study far exceeds the 36% that came out in a similar survey in 2008. The report further showed that 26% were investigating or planning to embark on an ERM program in the coming year. These responses according to Risk and Insurance Management Society (2011) suggest that ERM is becoming an accepted mainstream business discipline.

According to McShane et al., (2011) "traditionally, risk management has been compartmentalised and uncoordinated within a firm. Risk had been managed in silos with corporate risk managers focusing on pure risks (such as hazard risks), whereas the treasury department used derivatives to reduce financial risks, such as credit, market, and foreign exchange risk" (p.644). ERM attempts to address all risks, including additional risks such as operational and strategic risks and their coordinated efforts across the organisation as the risks may have a wider impact across the organisation than just a specific function or discipline. Arena, Arnaboldi and Azzone (2011) further explain that ERM is centred on the idea of risk management as a formal transversal process that addresses all those events that could prevent the achievement of corporate objectives.

Therefore, characteristics that distinguish ERM from siloed risk management are those of integration (taking a cross-functional, enterprise-wide perspective of risk, and embedding risk management throughout the organisation, its processes, and its culture), and strategic focus (the explicit positioning of the organisation's strategic objectives as the focal point for all risk encounters). To this effect, the emphasis on

ERM from both academic and business arenas has grown in the last decade, proposing ERM as a new instrument to predict risks and help organisations achieve their goals (Arena et al., 2011). However, it is not clear what impact this ERM shift has on the internal control system of an organisation as internal control encompasses the policies, processes, tasks and behaviours that enable an organisation to respond appropriately to risks (Ionescu, 2008). Internal control scope is supposed to cover the organisation's entire spectrum of operations and activities, not just those that are directly related to financial operations and reporting, as it has been the focus in a traditional risk management setting (Rae et al., 2008).

Furthermore, internal control environment itself has experienced challenges in the coordination and prioritisation of controls, leading to organisations having too many controls to address some risk areas, and not enough controls to address others and the duplication of controls (Ionescu, 2008). This raises questions as to whether the shift towards enterprise-wide risk management has led to improved integration and effectiveness of the control environment across the organisation.

Ionescu (2008) suggests that every organisation has different internal control requirements, circumstances and objectives, and that the ERM application also will vary depending on the organisational contexts. Jokipii (2010) found that this statement is corresponding to the contingency theory that claims that contingency characteristics of an organisation's size, structure, culture and the industry in which it operates influence how risk and control systems are applied within organisations. Therefore, this research sought to focus on the context of an industry, specifically the mining industry. The selection of this industry is informed by the reasons presented in the subsequent paragraphs.

The mining industry has played and continues to play a significant role in boosting economic growth, both globally and in South Africa. Creamer (2012) in his Mining Weekly article, reports that the global mining industry drives more than 45% of the world's gross domestic product (GDP).

In South Africa, the mining sector is the cornerstone of the economy; making a significant contribution to economic activity, job creation and foreign exchange earnings (Kearney, 2012). "Presently, South Africa holds some of the richest mining reserves on the globe, with a total value worth approximately US\$ 2.5 trillion, granting it the fifth largest mining sector in terms of GDP value" (Donovan, 2013, para.4). The industry accounts for about 18% of the GDP and roughly one-third of the market

capitalisation of the Johannesburg Stock Exchange, and continues to act as a magnet for foreign investment in the country (Kearney, 2012). However, the global mining sector has experienced dramatic changes over the past few years. While the industry is governed by risk management compliance requirements, with particular emphasis on safety risk management, the shifting social, economic and political trends have changed the operating efficiency of mining organisations (Deloitte, 2012).

A sustained period of high commodity prices has been followed by falling industrial demand for raw material inputs, constraints on access to capital, recent sharp corrections in all commodity prices and the ensuing need for reassessment of corporate strategies are some of the issues that the mining sector is faced with (PricewaterhouseCoopers, 2013). According to Deloitte (2012), issues around sustainability, the environment and human rights have escalated into more frequent episodes of labour unrest and community activism. Furthermore, while changes to government policy have been occurring for years, their volume, unpredictability and associated costs are escalating. Vecchiatto and Seccombe (2013) have also reported that about two-thirds of South Africa's platinum mines are making losses and a number of smaller companies have shut shafts or stopped production altogether. Furthermore, more than half of the country's gold mines are unprofitable.

Deloitte (2012) points out that these challenges troubling the industry are rapidly reaching an unprecedented level of extremity, which have necessitated a more robust and integrated approach to risk management. The mining companies are now placing increasingly higher priority on the need for effective corporate risk management. This paper, therefore, evaluates how the status of enterprise risk management in these organisations is affecting their internal control environment that is vital in helping them achieve their strategic objectives.

Controlling risks to maximise business objectives is not a new phenomenon. In order to explain the phenomenon, this paper borrows a quote from KPMG (1999, p16),

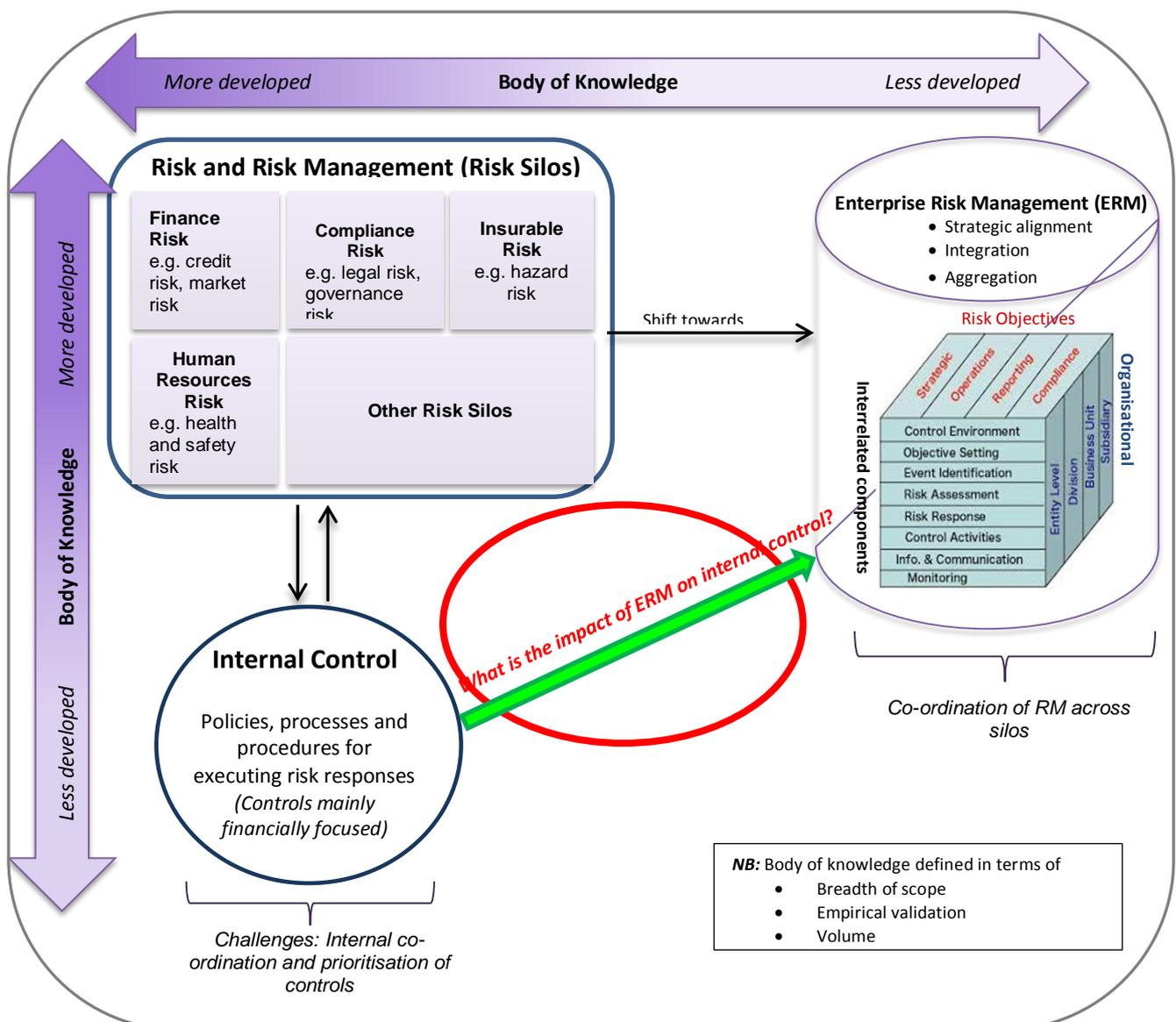
*"The business **objective** of a nineteenth century coal miner was to maximise coal output. More tonnage meant more money. Unfortunately, there was always the danger that the mine workings would collapse, delaying output and injuring, if not killing, the collier. This is the risk which threatened the achievement of the miner's objective. Fortunately, the miner could use pit props to **control** or manage the risk of collapse. For our miner, the secret of successful **risk management** was to maximise his time at the coalface by utilising the right number of controls. Too many props (over-controlled)*

would leave little time to dig coal. Too few props (under controlled) would result in disaster”.

1.3 Research Motivation

The research is driven by three factors. First, is the need for the academia to understand how the internal control of an organisation has been impacted since the advent of ERM framework. While Rae et al. (2008) suggest that further research in this area is especially needed as the benefits of having adequate internal controls have become clear, available knowledge base on both ERM and internal control is less developed. Figure 1 below, is a conceptual diagram that provides a summary of the current scope and the extent of research on the subject matter, highlighting the research gap in a red circle.

Figure 1: Summary of the current scope and the extent of research



The knowledge base on the implementation of ERM is less developed than for risk and risk management in general, characterised by the lack of empirical evidence on the effectiveness of ERM programmes (Arena et al., 2011; Gates, Nicholas, & Walker, 2012; Hoyt & Liebenberg, 2011; McShane et al., 2011). This is represented by the shaded bar at the top of Figure 1. Similarly, Selto and Widener (2004) analysed published research and found that there were fewer internal control topics in the internal control research literature, represented by the shaded bar on the left side of the diagram. Jokipii (2010) also found that the professional literature on internal control has made progress towards developing international control frameworks, but the amount of internal control research is limited. In addition, research on internal controls and risk management has focused mainly on maintenance of effective internal controls over financial reporting (Cappelletti, 2009; Doyle, Ge, & McVay, 2007; Gupta, 2008).

Secondly, this research was propelled by other researchers' studies which have thus far focused on exploring relationships between related internal control components (Rae et al., 2008) and relationships between risk management and internal control as it relates to financial reporting (Cappelletti, 2009; Doyle et al., 2007; Gupta, 2008). This research examines the unexplored relationship between enterprise-wide risk management (ERM) and internal control system, with the aim of determining the impact of ERM on the internal control of an organisation.

Lastly, in their report, PricewaterhouseCoopers (2007) affirm that an internal control system is one of the key management instruments at an organisation's disposal. Yet, Rae et al. (2008) found that the design of effective internal control systems remains a key challenge for senior management. Therefore, this research sought to determine how adopting ERM enables organisations to design and manage effective internal controls.

1.4 Research Objective

The research aims to understand how the ERM approach adopted by organisations in the mining industry has impacted their internal control system, which in turn is implied to help organisations to meet their strategic objectives, thus improving performance. Therefore the overall research objectives are to:

- Explore the extent to which organisations have adopted a formal enterprise-wide approach to risk management (ERM)
- Establish why organisations have adopted ERM

- Determine how this ERM adoption impacts the internal control of an organisation
- Identify key factors that are critical in ensuring a positive impact of ERM on an organisation's internal control system
- Provide insights that will bolster a successful advancement of internal control management through ERM.

1.5 Scope of Research

The research is limited to organisations within the mining industry which have some form of enterprise-wide risk management process in place. This selection was informed by the contingency theory arguments presented by Sarens and Christopher (2010) that companies operating in a complex industry such as mining are expected to have more developed risk management and internal control systems, which should allow them to compensate for the high volatility and low predictability that characterises complex industries. Whilst this research will contribute to the risk management and internal controls body of knowledge, the research will be limited to the geographical area of South Africa.

The research uses themes built from a synthesis of the literature to create a framework in order to facilitate the data collection and analysis, but remains open to emergent themes as the research progresses. This is done through an exploratory analysis based on semi-structured interviews with top management of the mining organisations, who are tasked with risk management, assurance of internal controls and those driving the attainment of strategic objectives of the organisation.

1.6 Organisation of Research

The remaining parts of the research report are structured as follows: Chapter 2 presents definitions of constructs and the literature related to the research questions. Chapter 3 outlines the main research questions. This will be followed by description of the research methodology in Chapter 4. Chapter 5 presents the findings of the research. The results are then discussed in Chapter 6. Here the results are discussed in terms of the research questions and the literature. In conclusion, Chapter 7 pulls the results together into a cohesive set of findings and provides recommendations for further research to be undertaken.

CHAPTER 2: LITERATURE REVIEW

The literature that contributes to the relationships between the constructs is presented in this chapter, giving insight into the theory surrounding enterprise risk management and internal control in the context of organisations. The chapter commences with evolution of ERM, how it differs from traditional risk management, its adoption in commercial organisations and those in the mining industry. This is followed by an overview of the role of internal controls, with specific focus on the significance of risk management in the internal control system. The various leadership and functional responsibilities for risk and control management are outlined and the challenges faced by both internal control and ERM implementation are highlighted. The chapter then reviews both the Contingency and Institutional Theory arguments about risk and control. Conclusions from the literature will then be drawn and brought to the fore.

2.1 The Evolution of Enterprise Risk Management

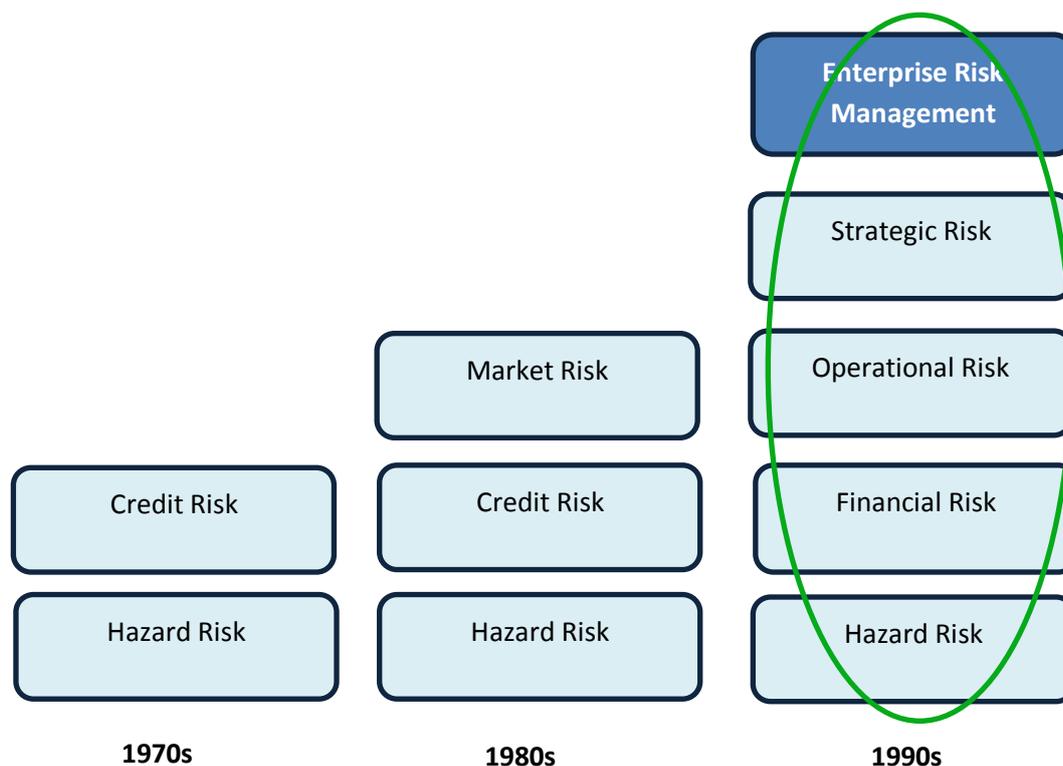
Bernstein (1998) explains the notion that during most of history, humankind had no more than a gut feel when faced with uncertainty. This changed dramatically in the 1600s when mathematics was applied for the first time in games of chance. The discoveries that followed gave strong foundations to the insurance industry and promoted the development of the field of risk management. Business could finally make rational assessments and develop suitable plans to manage unacceptable levels of risk. ERM has emerged as one of the features of the global explosion of this risk management industry, which began in the early 1990s initially in the financial services and insurance industries (Dickinson, 2001).

The explosion was initiated by regulatory and shareholder concerns over the governance of banking institutions in the late 1980s, the derivatives disasters of the early 1990s and the corporate scandals of the early 2000s, marking a promulgation of regulatory, academic, and practitioner dialogue around risk and risk management. Faced with institutional pressures to demonstrate improved governance and internal control, the financial industry saw a rapid evolution of ideas, processes, practices, and tools under the umbrella of integrated, holistic, enterprise-wide risk management Dickinson (2001). This promulgated into other industries.

Noting Figure 2 in the following page, risk management traditionally focused on financial risk (credit and market risks) and hazard risk. In the 1990s, approaching risk

from an enterprise-wide perspective began to be considered and implementation of ERM began. Examples of these types of risks include: (1) *Financial Risks*: includes risks from volatility in foreign currencies, interest rates, commodities, credit risk, liquidity risk, and market risk; (2) *Hazard Risk*: risks that are insurable, such as natural disasters, various insurable liabilities, impairment of physical assets, terrorism; (3) *Strategic Risk*: examples include risks related to strategy, political, economic, regulatory, and global market conditions; also could include reputation risk, leadership risk, brand risk, and changing customer needs; (4) *Operational Risks*: risks related to the organisation’s human resources, business processes, technology, business continuity, channel effectiveness, customer satisfaction, health and safety, environment, product/service failure, efficiency, capacity, and change integration (Shenkir & Walker, 2011)

Figure 2: Evolution of Risk Management into Enterprise Risk Management



Note: Adapted from Shenkir and Walker (2011)

While the implementation of ERM continued to grow and promulgate into various industries, the two prominent critics of ERM, David Martin and Michael Power, announced in 2007 the “end of Enterprise Risk Management” (ERM). They suggested that the practice is a “poor descriptive and normative model” that has less to do with managing risk and more to do with serving the professional interests of accountants

and regulators (Martin & Power, 2007, p. 9). They predicted the death of ERM in its form. However it has not been the case. The recent dialogue, following the topical global financial crisis of 2008-2009, has generated renewed regulatory and corporate interest in risk management, corporate governance, internal control, and the promotion of ERM as the “new paradigm” for risk management is respectively at an unprecedented high (Acharyya, 2006; Beasley, Branson, & Hancock 2011; Blaskovich & Taylor, 2011; McShane et al., 2011).

Despite the intense concern of government and stock exchange activities related to risk management within corporations, academic research in this area is not as intense. Research has been done to study the aspects of whether ERM adds value to organisations (Gates et al., 2012; Gordon, Loeb, and Tseng 2009; Hoyt & Liebenberg, 2011), however, there is lack of empirical evidence to suggest the effectiveness of the ERM programmes. Even more so, from a South African perspective, particularly in mining, the ERM literature is almost non-existent.

2.2 Differentiating Traditional Risk Management and Enterprise Risk Management

Following Rao's (2007) definition, the term "risk" includes any event or action that will adversely affect an organisation's ability to achieve its business objectives and execute its strategies successfully. At any given time, an organisation is exposed to multiple sources of risk such as future events, issues or scenarios which may potentially have an impact on the achievement of the company's objectives, some being unavoidable or inherent in the nature of the organisation's operations and environment, and some arising from deliberate business decisions. While Vijayakumar and Nagaraja (2012, p. 2) describe risk similarly to Rao's (2007) definition as “the possibility of an event occurring that will have an impact on the achievement of objectives”, they further explain that “It is measured in terms of impact and likelihood, further; it can be both threats and opportunities which may be exploited” (p. 2).

Historically, the management of these risks has been done in silos; risks such as insurance risk, financial risk, market risk, hazard risk, and technology risk were all managed independently in separate compartments, even though there might be some risks related to each other that may affect each other (Hoyt & Liebenberg, 2011; Rao, 2007). Risks, and the treatment strategies employed to manage one set of risks, may exacerbate or mitigate other risks. Such interdependencies mean that the “siloes” management of risks may result in sub-optimal outcomes at the enterprise level; risks

considered acceptable when assessed independently may result in an unacceptable level of risk when considered together. Furthermore, the coordination of risks has usually been non-existent, and the identification of new risks has been lethargic (Rao, 2007).

As the economic and business landscape changes due to forces of globalization and the geopolitical environment in which organisations operate in, a variety of more risks confront organisations. This increasing risk environment requires that senior management adopt enterprise risk management (Barton, Shenkir, & Walker, 2010). Beasley et al. (2011) describe ERM as a formal process that is enterprise-wide and that addresses risks in a portfolio manner, where interactions among risks are considered. The goal of ERM is defined by McShane et al. (2011, p. 644) as “the coordinated management of all risks faced by a firm, whether it is risk related to corporate governance, auditing, supply chains, distribution systems, IT, or human resources,...with a purpose of gaining a systematic understanding of the interdependencies and correlations among risks”.

From this it can be said that the sources of enterprise risk solutions are many; from the qualitative world of audit and control, the actuarial world of insurance and risk management, the six sigma world of quality and engineering risk management, to the quantitative world of financial, market and credit risk management. It is evident that each set of solutions speaks a different risk management language as Hoyt and Liebenberg (2011) have pointed out. These multiple languages of risk all need to be translated to the one language that is relevant to management. This can be achieved through ERM.

Nocco and Stulz (2006) further distinguish the multi-dimensional nature of ERM from the traditional isolated risk management activities. Firstly, ERM takes a holistic, cross-functional and integrated approach, in contrast to the traditional management of risks in functional “silos”. Nocco and Stulz (2006) elaborate further that an organisation can manage risks in one of the two different ways; one risk at a time, on a predominantly compartmentalised and decentralised basis; or all risks viewed and managed together within a coordinated and strategic framework. The idea is to have an Enterprise Risk Profile, an aggregate representation of an organisation’s risk universe, accounting for all types of risk exposures within the organisation, across different business activities and risk types, and for the inter-relationships between those exposures. The Enterprise Risk Profile represents an idea that the (known) universe of likelihoods potentially affecting an organisation’s future performance can be recorded and meaningfully

interpreted by those making decisions. Therefore, ERM represents the state of knowledge essential to make globally efficient business decisions (Rao, 2007). Alviniussen and Jankensgård (2009) elaborate that “The Total Risk Profile of a company is highly related to and a function of corporate policies and strategic decisions” (p. 179).

Another distinguishing feature of ERM is the idea of embedding risk management throughout the organisation and its processes, as a culture, rather than as an additional “bolted on” bureaucratic task. Kimbrough and Compton (2009) and Shenkir and Walker (2006) found that risk management is more effective and efficient when it is carried out as an integral part of organisational processes, rather than as an added extra that people have to accommodate on top of their normal workloads. ERM promotes a risk-aware culture where people are aware of and understand risk in the context of the organisation’s objectives, where all decisions in the organisation, from strategy setting to operations, involve the consideration of risk, and where risk management procedures and tools are employed in day-to-day activities of all staff (Shenkir & Walker, 2006).

ERM therefore makes possible the aggregate view of potential future impacts on the achievement of the organisation’s objectives arising from all identified sources of risk across the organisation. A core element of ERM is that risks and strategy are aligned and are integral to strategic planning and performance assessment (Beasley et al., 2011). Below is a summary table of the key differentiators between ERM and traditional risk management.

Table 1: Key features of ERM versus traditional risk management

Traditional risk management (TRM)	Enterprise risk management (ERM)
<ol style="list-style-type: none"> 1. Fragmented – department or function manage risk independently; accounting, treasurer, internal audit primarily concerned 2. <i>Ad hoc</i> – risk management done whenever managers believe a need exists to do it. 3. Narrowly focused – primarily insurable risk and financial risks 	<ol style="list-style-type: none"> 1. Integrated – risk management coordinated with senior-level oversight; everyone in the organisation view risk management as part of their jobs. 2. Continuous – risk management process is on-going 3. All business risks and opportunities considered within organisation’s risk appetite - Strategic objectives are the focal point for all risk encounters.

Note: Adapted from Rao (2007)

2.3 Adoption of ERM as business imperative

Economic markets, both global and domestic continue to become more complex, creating challenges for senior executives and boards of directors who provide strategic leadership and governance oversight for the organisations they serve. Beasley et al. (2011) acknowledge that “an increasing number of business leaders are realising that traditional approaches to risk management require enhancement so that they are in a more-informed position to proactively manage emerging risks, especially those that are most likely to disrupt organisational objectives” (p. 2). However Arena et al. (2011) found that ERM still means different things to different people. For instance to others it is just a compliance/ tick-box exercise, to others a corporate governance requirement and others an instrument that can help an organisation to manage its risk.

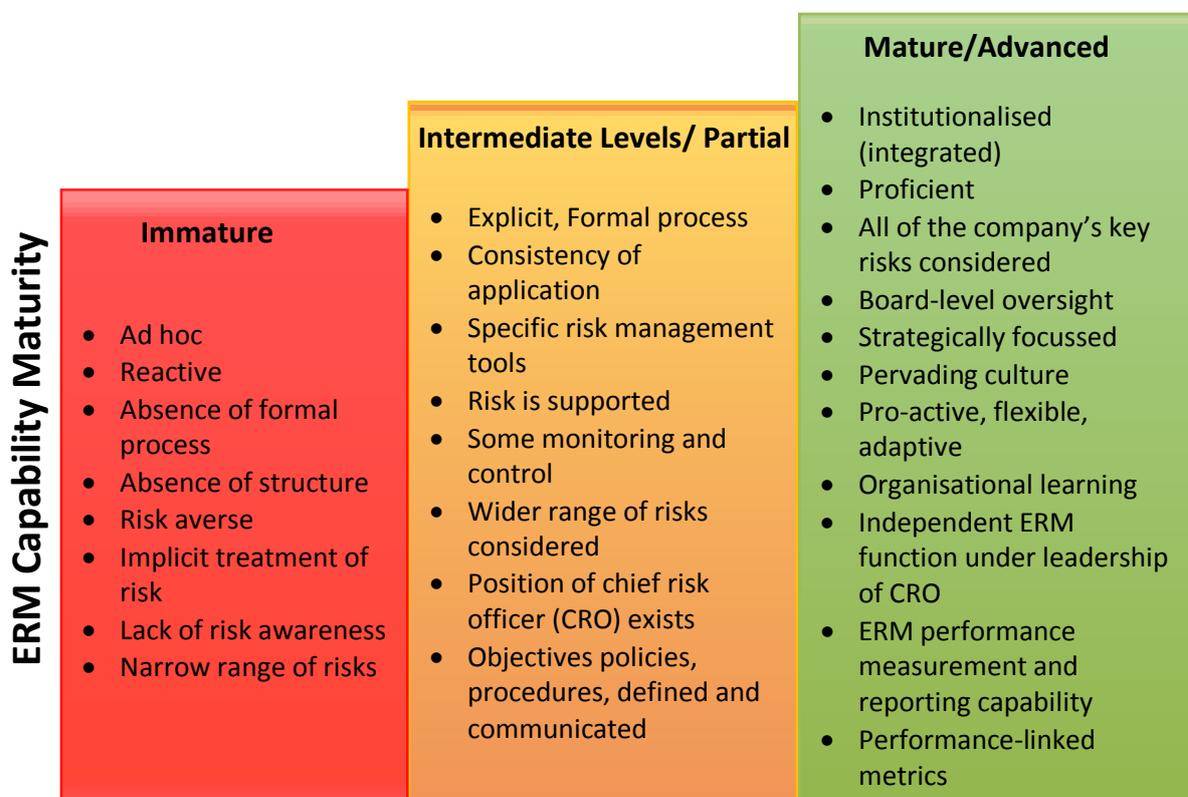
Even so, a study by Beasley et al. (2011) revealed a modest trend towards more advanced enterprise-wide risk oversight from 2009 through 2011. The study found that despite the growing demand for more effective risk oversight that has emerged from the recent financial crisis, the level of enterprise-wide risk oversight across a wide range of organisations remains fairly immature. Beasley et al. (2011) attributed this to the challenges that organisations face when implementing enterprise-wide risk management. Achieving greater penetration and integration of risk management into business processes, facilitating a risk-aware culture, measuring and aggregating risk (particularly non-traditional risks such as emergent risks in supply chain, vendor, geo-political environment) and developing tools and systems to support risk management are some of these challenges.

Coetzee and Lubbe (2013) on the other hand found in their study that South African private sector organisations listed on the Johannesburg Stock Exchange (JSE) are on average risk mature, with thirty out of the forty organisations in the sample being risk mature. Could this mean that risk management practices in South Africa are more mature compared to their global counterparts?

In assessing the level of adoption or maturity of ERM processes within organisations, there are various Capability Maturity (CM) models for benchmarking the maturity of ERM. In principle, the CM models describe capability maturity on a scale ranging from practically non-existent, to fully integrated and proficient levels (Beasley et al., 2011; Shenkir & Walker, 2011; Coetzee & Lubbe, 2013; MacGillivray, Sharp, Strutt, Hamilton, & Pollard, 2007).

Figure 3 below shows typical descriptions of enterprise risk management process maturity.

Figure 3: Typical descriptions of enterprise risk management maturity



At the initial stages of immaturity, ERM is either non-existent within the organisation, or performed only on an ad hoc basis. There is no formal process or practice to cross-assess the organisation's risks thus, providing a narrow view of risks. A more enterprise level risk management is adopted at intermediate levels; risk management is an explicit and formal process within the organisation and is consistently applied, with support from senior management. The role of CRO exists and a wider range of risks is considered. The risk management processes reach maturity or more advanced when they become integrated as a proficient capability throughout all business processes, are tied to the organisation's strategic objectives and are dynamically adaptive to the needs of the organisation. At this level, risk management pervades the culture of the organisation, is almost intuitively pro-active rather than reactive, and continually evolves as organisational members learn from experience, training and education (Beasley et al., 2011; Coetzee & Lubbe, 2013; Shenkir & Walker, 2011; MacGillivray et al., 2007).

Capability Maturity models describe the characteristics of effective enterprise risk management, but the definitions are not necessarily grounded on sound empirical analysis of actual risk management processes in organisations (see section 2.1 above). These models, as a result, appear to derive their process definitions and characteristics from translation of the principles of ERM as outlined in the various risk management frameworks such as ISO 31000 (2009) and the COSO (2004) Enterprise Risk Management-Integrated Framework.

2.3.1 ERM adoption in a complex industry driven by governance factors

Mining, in recent years, has been the single most dynamic component of many countries' total productive activity. Thus it has become a potential catalytic force for faster overall economic growth of nations. The industry is a bellwether for the global economy (Hermanus, 2007). When mining started on an industrial scale in the 1880s, miners faced very high levels of risk to both safety and health. Hermanus (2007) points out that over the years the safety performance of mines has improved, but not at the same rate as at in other major mining countries such as Australia, Canada and the USA when comparing South African mines. Boegman (2013) emphasises that it is imperative that mining companies rethink risk and the risk landscape in which they operate, and gone are the days when risks for mining companies were limited to health and safety matters.

Mining companies now need to integrate risk and performance management and they need to evolve risk management to be more predictive in order to anticipate and plan for negative potential events. Deloitte (2010) concurs that whilst some traditional risk management approaches may have served the industry well in the past, the scope, complexity, and interdependencies of emerging risks are forcing many energy and resources companies to adopt comprehensive and integrated approaches to risk management. Refer to Appendix 1 for types of risks mining organisations are faced with.

Heuberger (2005) found that the mining industry has not become less risky over the years. In fact, it has become more uncertain. Even so, from a South African perspective, policy uncertainty, for example resource nationalism, could have a significant impact on the operational performance of mining companies operating in South Africa. The industry is rocked by problems concerning retrenchments, unemployment, low productivity, rising costs, volatile exchange rates, commodity prices and government regulations (Heuberger, 2005).

The global mining industry is highly regulated. It operates under legal and fiscal frameworks linked together by various national, regional and commodity-focused associations committed to representing the industry, protecting its interests and improving performance (International Council on Mining and Metals (ICMM), 2012). Each jurisdiction publishes information that summarises key aspects of its mining law and administration. Noncompliance with regulatory requirements could result in forfeiture of mineral rights. Furthermore, mining is a hazardous activity. Apart from personal suffering, work-related injuries could lead to a shutdown of operations resulting in lost production and jeopardise the company's licence to operate.

Besides the higher complexity and difficulty of having a clear overview of risks in larger organisations, regulations tend to require reporting on risk management in the annual statements. Example of such regulations are the requirements of the South African King III report on Corporate Governance, which have resulted in improved disclosure of risks by all companies. According to Boegman (2013), mining companies in particular have been good at disclosing these risks. The regulatory, political and legal environment, followed closely by employee skills and safety are amongst the most common risks disclosed by the companies (Boegman, 2013). However, the challenge remains to adequately embed ERM in the mines' operations, thus taking a holistic, company-wide approach to managing a company's risks.

2.4 Defining Internal Control and its role in the organisation

Vijayakumar and Nagaraja (2012) explain that internal control is one of the several factors influencing the performance of an organisation. They say it plays a vital role in achieving the organisation's intended objectives and it is fundamental to the successful operations. Dietz and Snyder (2011) further unpack internal controls as processes, policies, procedures and systems that are established, operated and monitored by officers responsible for governance and management of the organisation, to provide reasonable assurance regarding the achievement of the organisation's objectives. Therefore, 'internal control' and 'internal control system' are used interchangeably.

Jokipii (2010) explains an internal control system as a structure with five components as follows:

1. The control environment component defines the ethos of an organisation and the way it operates. This component refers to the creation of an atmosphere in

which staff can conduct their activities and carry out their control responsibilities. It creates the overall control culture in the firm.

2. The risk assessment component refers to the processes of dealing with the risks that pose a threat to achieving the firm's objectives. It involves the identification, analysis and assessment of relevant risks.
3. The control activities component refers to the policies, procedures and practices that assure management that objectives are achieved and the risk mitigation strategies are carried out effectively.
4. The information and communication component ensures that relevant information is identified, captured and communicated in a form and time frame that allows staff to carry out their duties and responsibilities effectively.
5. The monitoring component refers to a process of assessing the quality of control. It covers on-going and periodical evaluations of the external supervision of internal controls by management or other parties outside the process.

Vijayakumar and Nagaraja (2012) and Dietz and Snyder (2011) summarise the main purpose of effective internal control as managing risks, protecting assets of an organisation, deterring fraud, and improving compliance.

As mentioned in Chapter 1, the increasing number of business failures and some widely publicized frauds have encouraged firms to put more emphasis on their internal control systems. Jokipii (2010) notes that management is under increased pressure to enhance the effectiveness of internal control and to effectively communicate this to the board of directors and shareholders. Auditors, suppliers and customers of organisations are also interested in internal controls since they may affect long-term confidence in reporting, accountability and in the corporate form of organisation.

Jokipii (2010) further argues that despite the fact that internal control is an essential factor affecting the organisation, evidence of the actual performance of an internal control system within the organisational environment is almost non-existent and that the topic is relatively unexplored by researchers, even more so for the mining industry (Giriunas,2012). The existing research in internal controls and risk management literature has focused mainly on maintenance of effective internal controls over financial reporting (Cappelletti, 2009; Doyle et al., 2007; Gupta, 2008; Power, 2009). Furthermore, Lin and Wu (2006) and Blaskovich and Taylor (2011) found that in the audit literature, the concept of internal control is narrow in scope as it is largely confined to accounting systems to support the accounting process. They maintain that

auditors do not generally concern themselves with controls beyond the accounting process and this is where the problem of the traditional internal control concept lies.

They further allude that the reasons why the internal controls movement does not have a thriving tradition of controls design to include enterprise-wide risks is because the controls movement has been led by auditors, and auditors do not design controls or processes, they audit internal controls based on prescribed accounting standards.

2.4.1 Significance of Risk Management in the Internal Control System

As explained in the previous section, the subject of internal control has traditionally been debated as a procedural system intended to ensure reliability of financial reporting and was triggered by fraudulent financial reporting. However its concept has been clarified since the 1990's and has been purported to be essential for organisations to reduce risks concerning the achievement of its objectives and pursue lasting growth. Risk management on the other hand developed initially from the viewpoints of natural disaster preparedness and the management of finance-related uncertainty. However, the concept of risk management is today taken as activities intended to manage wide-ranging risks, in response to the increasing need of managing socioeconomic uncertainty. Although risk management and internal control emanate from different backgrounds and have been developed through different paths, they have numerous common objectives, deal with various risks surrounding business landscape and work to maintain and enhance the value of the organisation.

In recent times, as environments surrounding organisations are changing and the responses thereto of the companies are exposed to more stricter criticism from markets, it has become necessary to associate enterprise risk management with internal control and understand how they relate to each other. Mikes and Kaplan (2013) point out that the common thread in the recent corporate governance reforms such as the Turnbull report in the United Kingdom, the COSO Enterprise Risk Management Framework, ISO31000 and other American-based regulations is that they all frame risk management as a corporate governance requirement, implying a relation with internal control. The Sarbanes-Oxley Act of 2002 Section 404, explained by Securities and Exchange Commission (2009) and the South African King III Report on Corporate Governance (Institute of Directors, 2009) also relate risk management to internal control, implying a risk-based assurance of internal control.

As indicated in Chapter 1, Rae et al. (2008) point out that as a result of these recent reforms, organisations in the various sectors are faced with a growing number of

options for managing the internal control system, including the adoption of enterprise risk management (ERM). Cappelletti (2009) also makes reference to the use of ERM to improve internal controls. According to Rae et al. (2008), these various corporate governance guidelines have also placed significant emphasis on an organisation's approach to risk management as a key mechanism that overarches the design of internal controls throughout the organisation.

Authors including Vijayakumar and Nagaraja (2012) and Ionescu (2008) purport that risk management forms an integral part of internal control. Ionescu (2008) explains that risk management is essential for reducing the probability that corporate objectives will be jeopardised by unforeseen events. Organisations should therefore determine the type and extent of risks that are acceptable to them and strive to maintain risk within these levels. In doing so, internal control is one of the principal means by which risk is managed.

Vijayakumar and Nagaraja (2012) assert that internal control comprises the process of defining all risks that an organisation faces and then building a framework, not only to monitor and mitigate those risks but also to use risk management as a tool to increase shareholders value. An organisation's objectives and the environment in which it operates are constantly evolving and as a result, the risks that it faces also change. A sound system of internal control depends on a thorough and consistent evaluation of the nature and extent of the risks to which the organisation is exposed. The systems and processes of control need to be adequately flexible to be able to change and adapt as the environment and the organisation's objectives and activities develop over time.

The authors point out that since profits and increases in shareholder value are in part, the reward for successful risk taking in business, the purpose of internal control is to help manage and control risk appropriately, rather than to eliminate it. Put simply, internal controls help to provide reasonable, but not absolute, assurance that a company will avoid being hindered in achieving its business objectives, or in the systematic and legitimate conduct of its business, by circumstances that may reasonably be foreseen. Specifically for the mining industry, the changing subjects of political, economic, social and technological aspects affect the policy and management of organisations in the mining industry. Therefore, given the changing conditions, internal controls may become inappropriate or even ineffective; therefore, the effectiveness and overall management of these internal controls is paramount in enabling the achievement of the organisation's strategic goals (Giriunas, 2012).

2.4.2 Challenges in the management of Internal Control

As outlined in the problem statement in Chapter 1, internal control environment has experienced challenges in the coordination and prioritisation of controls. Ionescu (2008) summarises some of the reasons why organisations have remained stuck in inefficient control environments as follows:

- Duplication of risk and control activity - Significant effort and costs are expended by organisations to build controls that address potential risk. However, in most cases the correlation, intersection and duplication of controls across different groups are not clearly visibly or easily understood because of the siloed approach that many organisations have taken in the past towards risk management. This results in cost inefficiencies. In order to avoid or minimise these outcomes, an enterprise-wide view of risk is required.
- Too much of some controls, not enough of others - Most organisations have too many controls to address some areas, and not enough controls to address others. Internal control activities tend to be added over time, but not taken away or reduced when the need has been served.
- Prioritisation of controls - Furthermore, decisions on which critical controls should be focused on becomes a challenge when not addressed at enterprise level and this results in inefficient resource allocation.

The challenges presented above indicate that there is scope for ERM to help avoid or overcome these challenges.

2.5 Responsibilities for ERM and Internal Control

Blaskovich and Taylor (2011) outline that the organisation's board of directors is ultimately responsible to ensure that the company maintains sound and effective internal controls based on comprehensive risk management to safeguard the shareholders' investment. The corporate governance guidelines mentioned in section 2.4.1 above suggest where applicable that the board also disclose any significant failing or weakness in internal control and its impact on the company, enabling investors and the public to appraise the position of the company. The board delegates the responsibility for owning and managing risk with the Chief Executive Officer (CEO), and, by delegated authority, with executive and line management of the organisation. Rae et al. (2008) also point out that the responsibility of implementing an effective

ERM framework lies with management, of which the design of the internal control system is a vital aspect.

As explained by Acharyya (2006), Chief Risk Officers (CRO) or the person in charge of risk management, commonly have responsibility for deploying and implementing the overall risk management policy and process agreed upon by the organisation's board and senior management. For this purpose, he or she establishes a structured system that is both permanent and adaptable for the purpose of identifying, analysing and managing the main risks. They run the risk management system and provide methodological support to the company's line and staff divisions, and may even have significant power, with CEO's delegation in risk allocation decisions.

Traditionally, the internal audit function's role has been to assess the effectiveness of organisational internal controls, and to report to management where and how internal controls could be strengthened. Such assessment of internal controls (also called assurance) is an integral part of a company's system of internal control and helps to ensure its effectiveness (Vijayakumar & Nagaraja, 2012). Since the advent of ERM, internal auditors have been encouraged to take on a new and potentially more valuable role in their organisation's approach to ERM (Rae et al., 2008).

This includes following a risk-based approach to internal audit as it allows internal audit to determine whether controls are effective in managing the risks which arise from the strategic direction that a company, through its board, has decided to adopt and providing assurance on the risk management processes. Baker (2013) found however, that most internal audit functions have been successful in providing broad advice on risk management, but few of them are confident enough to provide specific assurance and recommendations on more advanced enterprise risks to move risk management ahead in their organisations and ensure effective system of internal controls.

The management of risk and internal control in the organisation can therefore be seen as divided into three functions: (1) the taking of risk, undertaken by the organisation's board and the management of system of internal control, is driven by the CEO; (2) the observation and support of risk management, is undertaken by the office of the CRO; and (3) the monitoring and audit of risk management and associated internal control, is undertaken by the office of the Internal Auditor.

For this to succeed, Coetzee and Lubbe (2013) argue that that without the buy-in of the governing body, as the overseers of the framework, and senior management as the initiators of the implementation, risk management cannot be successful. Unfortunately,

research has indicated that although in many instances management perceives risk management as an excellent tool to assist in managing crucial risks threatening the organisation, it is also sometimes perceived as something that must be done simply to demonstrate compliance with applicable guidance and legislation.

2.6 Contingency and Institutional Theory interpretations of risk and control

Available research has mainly focused on the influence of contextual variables on internal control structure and risk management of an organisation (Ionescu, 2008; Jokipii, 2010) and in this paper, the literature is reviewed. However, the aim is to use contingency theory to understand the internal control and its observed effectiveness in the advent of ERM, rather than to elaborate on contingency theory as such. Furthermore, the findings of this research will need to take into consideration the contingency arguments presented by the authors that every organisation has different internal control requirements, circumstances and objectives, and that the ERM application also varies depending on the organisational contexts.

Coetzee and Lubbe (2013) explain that risk management is not a simple concept and the reason is that each organisation develops its own, usually unique framework, consisting of different practices and activities. Organisations thus determine the quality and the quantity of activities to be implemented in order to determine whether risks are appropriately managed according to the wishes of its governing bodies and senior management, and whether the risk management process is in line with what is communicated to its stakeholders. Contingency characteristics of an organisation's size, culture and the industry in which it operates influence how risk and control systems are applied within organisations (Jokipii, 2010).

The impact of these external and internal contingencies has also been recognised in institutional theory. Selznick (1996) explains that the institutionalisation process exists at two levels – that of the organisation with the external world and that of an organisation internally (often as a result of the external pressures). Gupta et al. (1994) notes that contingency theory and institutional theory, when applied separately, they only provide an incomplete understanding of the different roles played by various coordination and control practices that are used in contemporary organisations. Applied together, both theories could offer a better understanding of roles fulfilled by coordination and control practice.

Each of the contingency characteristics is explored below.

2.6.1 Organisation size

The earlier contingency research suggests that an organisation's size may affect the organisation's method of designing and using management systems (Hoque and James 2000). This view of contingency theory is used by Jokipii (2010), who argues that organisational growth increases communication and control problems and that when an organisation's size increases, its control processes become more specialized and sophisticated. Gupta et al. (1994) explained that size may be an institutional phenomenon in that larger organisations are more visible to a variety of external constituents and thus are subject to institutional pressures.

Sarens and Christopher (2010) further iterates that larger companies are expected to need more developed risk management and internal control systems to reduce the significant agency problems to which they often are subjected. However, it may take longer for these companies to develop such risk and control systems as size of the company and the number of geographical locations have an influence on how quickly these can be developed. An organisation size may be defined based on the number of employees, number of subunits, the number of clients served, sales, assets, profits and production volume (Jokipii, 2010). The same reasoning applies for companies with a larger number of reporting levels. For purposes of this research the size of the organisation is defined by number of employees.

2.6.2 Organisational Culture

Kimbrough and Compton (2009) found that in contrast to ERM, organisational culture has been a topic of management theory for several decades. The underlying thought is that organisational culture plays a critical role in how major initiatives are implemented, how quickly the organisation can react to market changes, and whether or not the organisation can successfully navigate major changes in the business environment. Since ERM is a significant initiative, and it is intended to help an organisation be more resilient in times of uncertainty, an organisation's internal culture is a significant factor in ERM deployment. This paper does not evaluate the impact of culture on ERM deployments; it offers a basis for understanding the cultural dynamics that play a significant role in ERM and internal controls management.

Kimbrough and Compton (2009) also found that culture is featured prominently in theoretical ERM frameworks, although words used to describe it vary. Others call it "organisational context" and in some literature it is called "risk culture". This paper follows on the organisational culture framework proposed by Kimbrough and

Componation (2009), linking ERM to the organic-mechanistic framework as follows: The shift from the tradition of managing risk within organisational silos to managing risks on a portfolio basis across the entire organisation leads to a requirement for effective communication and collaboration across the organisation. In addition, ERM assumes that identification and communication of risks will occur freely and that there will be “risk transparency throughout an organisation”. These qualities appear to align with the organic characteristics of collaboration, lateral communication, and employee commitment to the organisation’s tasks.

Simultaneously, definitions and frameworks portray ERM as a process that involves mechanistic qualities that advocate compliance with rigorous activities such as regular risk identification, analysis, prioritisation, monitoring, control activities, and the use of a common risk language. Adherence to such standards is usually mandated from as high as the board of directors. These attributes lean toward the mechanistic end, characterised by insistence on obedience to superiors, employees needing detailed instructions, and a hierarchical chain of command (Kimbrough & Componation, 2009). In order to reap the benefits of ERM more quickly, Kimbrough and Componation (2009) concluded that it is desirable for organisations to foster a more organic culture. They advise that organisations must lead the way by institutionalising enterprise risk management along with the supervisory and cultural elements that support ERM activities. Kimbrough and Componation (2009) note that studies have found organisational culture to be one of the top barriers to ERM implementation and that the importance organisational culture is emphasised as critical when deploying ERM programs.

2.6.3 Industry

The nature of the industry drives the nature of risks and risk management processes adopted to manage the risk. The context within which the organisation functions is taken into account when making reference to the nature of the industry. It is often referred to as either “simple” versus “complex” or as “dynamic” versus “stable” (Gupta, et al., 1994). Jokipii (2010) argues that the more complex and dynamic the external environment, the greater the reliance on formal controls. Furthermore as Sarens and Christopher (2010) have indicated, companies operating in a complex industry such as mining are expected to have more developed risk management and internal control systems, which should allow them to compensate for the high volatility and low predictability that characterises complex industries. The control system becomes more important when uncertainty is greater in industries such as mining.

Conversely, DiMaggio and Powell (1983) argue that there is a greater degree of organisational similarity, especially within the same industry, due to the existence of institutional isomorphism. They suggest that this is attributed to mandates by institutional regulation or uncertainty in the environment which may cause organisations to seek out and mimic those perceived as more successful and legitimate. Gupta (1994) alludes that because an organisation depends for survival on the support of external constituents, it must conform to institutionalised expectations or norms expressed in elements such as rules, regulations, blueprints for action, or standards.

From the literature provided, it is clear that ERM application and internal control management are contextual and take into consideration the organisation's size, structure, culture or type of industry. Mikes and Kaplan (2013) recently found that risk still means different things in different organisations and experience has taught risk managers that a given risk model will work in some contexts and not in others.

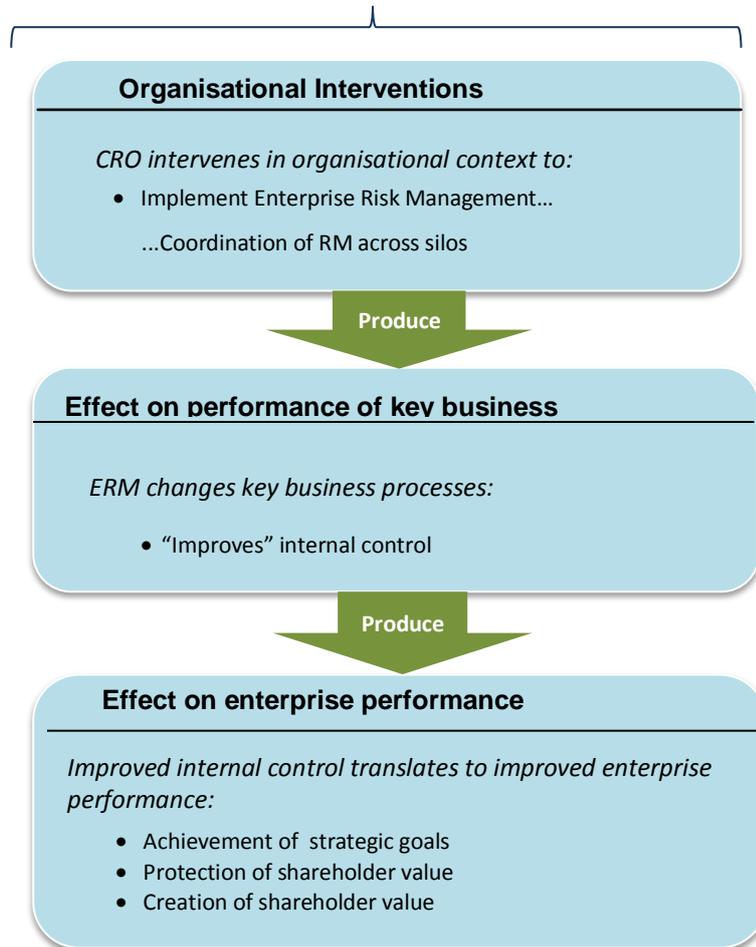
2.7 Inferences drawn from the literature

Ionescu (2008) and Vijayakumar and Nagaraja (2012) affirm that the Internal Control System is an integral part of the business processes at all levels of the organisation. It is a system established and operated in a company to carry out its business properly and efficiently. Internal control is at the same time essential for a company to reduce risks concerning the achievement of its objectives and pursue lasting growth (Arena *et al.*, 2011; Cappelletti, 2009; Gates *et al.*, 2012; Lin & Wu, 2006; Rae *et al.*, 2008; Vijayakumar & Nagaraja, 2012). Organisations in the various sectors are faced with a growing number of options for managing the internal control system and some have adopted ERM to improve their internal control (Cappelletti, 2009; Rae *et al.*, 2008). The literature has placed significant emphasis on an organisation's approach to risk management as a key mechanism that overarches the design of effective internal controls in the organisation. Based on the risk management literature, ERM approach theoretically provides a platform for improved internal control.

As shown in the summary diagram in Figure 4 in the following page, ERM interventions, informed by the organisation's context, enhance the internal control system, which in turn is implied to help organisations to meet their strategic objectives, thus improving performance.

Figure 4: Constructs Relationship diagram

Assumptions about the effects of ERM implementation on the organisation



From the contingency theory and institutional theory perspective, ERM application and internal control management are contextual and take into consideration the organisation's size, culture and the type of industry in which it operates. Assertions made by the literature are that companies operating in complex and dynamic industries such as mining are expected to have more developed risk management and internal control systems. The literature has not been explicit as to which key factors are critical in ensuring that ERM enhances the internal control of organisations.

2.8 Conclusion

It is evident from the literature that has been reviewed that academic knowledgebase of ERM and internal controls is limited. Even more so from a South African perspective, particularly in mining, it is almost non-existent. However guidance does

exist in the form of corporate governance guidelines that organisations can utilise to inform best practice application in a local context.

In summary, this chapter discussed the literature around the evolution of Enterprise Risk Management, how it differs from traditional risk management, its adoption in organisations and those in mining industry, the role of internal controls, the significance of risk management in internal control system, what the different responsibilities are for risk and control management, the challenges faced by both internal control and ERM implementation, and reviewed both the Contingency and Institutional Theory arguments about risk and control.

Built from these theoretical analyses are four themes that cover the adoption of ERM as a business imperative, the impact of ERM on internal control, key success factors to ensure ERM enhances the internal control system and the organisational context. These formed the basis of the research questions outlined in Chapter 3 and were utilised as a tool for guiding the data collection and analysis process, which is explained in Chapter 4. It is to be noted that of the four themes outlined above, the theme of organisational context does not form part of the main research questions, but is included in the data collection and analysis to take the contextual elements into consideration when evaluating the findings, as every organisation has different internal control requirements and ERM application also varies depending on the organisational context.

CHAPTER 3: RESEARCH QUESTIONS

The purpose of this research study is to explore the impact that ERM has on the internal control system of organisations in the mining industry, specifically determining if implementing ERM enhances the organisation's internal control system. The previous chapter discussed the available literature during which a few important themes surfaced. Chapter 3 emphasises these themes in the form of research questions that are explored in this research. Thus, these questions draw on issues that have emerged from the literature review detailed in Chapter 2, supported (and expanded) by the motivation for the research as detailed in Chapter 1, which this research study attempts to investigate.

Research Question 1: To what extent have organisations adopted a formal enterprise-wide approach to risk management and why did they adopt it?

Ionescu (2008) explained that every organisation is, to some extent, in the business of risk management, irrespective of what products or services the organisation delivers. As such effective risk management that spans the organisation should be a business imperative for any organisation that wants to survive in today's challenging global economy. Particularly, the complex nature and status of the mining industry requires an integrated ERM to be formally adopted as a business imperative (Jokipii, 2010). However, Arena et al. (2011) found that ERM still means different things to different people; to others it is just a compliance/ tick-box exercise, to others a corporate governance requirement and to others an instrument that can help an organisation to manage its risk.

In order to evaluate any impact that ERM may have on internal controls, it is important that this research establish the extent to which organisations have formally adopted the ERM framework and why they adopted it.

Research Question 2: How does ERM enhance an organisation's internal control system?

There are two assertions from the literature; firstly, there are existing conceptual arguments that an internal control system relies on the risk management system to identify the risks that need to be controlled. (Arena et al., 2011; Cappelletti, 2009; Secondly, an effective system of internal control rests on adequate and comprehensive analysis of enterprise-wide risks (Lin & Wu, 2006; Rae et al., 2008). Gates et al., 2012;

Vijayakumar & Nagaraja, 2012). The shift from the silo-based traditional risk management to ERM has therefore theoretically provided a platform for improved internal control. The literature implies that ERM improves internal control, which in turn helps an organisation to achieve its strategic objectives - the question is how?

This study seeks to expand these conceptual arguments by investigating these improvements brought about by ERM on the internal control of an organisation.

Research Question 3: What are the key factors that are critical in ensuring that ERM enhances an organisation's internal control system?

The literature has presented challenges faced by organisations when implementing and managing enterprise-wide risk management, and these include challenges around achieving greater penetration and integration of risk management into business processes, facilitating a risk-aware culture, measuring and aggregating risk (particularly non-traditional risks) and developing tools and systems to support risk management (Beasley et al., 2011; Kimbrough & Compton, 2009). The literature has not emphasised specifically on the key factors critical in ensuring that the deployed ERM approach enhances the internal control of organisations. If organisations are looking to ERM to improve the internal control system, advice should be given on what is critical to ensure the success.

The question asked by this paper seeks to find other factors that can affect the success of ERM in enhancing the internal control system of the organisation.

CHAPTER 4: RESEARCH METHODOLOGY

The previous chapter explained the research questions that were explored in this research study. The purpose of this chapter is to describe the research methodology that was used to gather and analyse the data for the questions outlined in Chapter 3.

4.1 Research design and rationale

The research, in its attempt to determine the impact that ERM has on organisations' internal control systems, was exploratory and qualitative in nature due to its 'interpretivist' view of reality. Interpretive or 'interpretivist' philosophy as explained by Myers (2013) aims to understand the context of a phenomenon and involves the exploration of a research topic or theory, rather than testing theory (positivist philosophy).

Saunders and Lewis (2012) recommend the use of qualitative study if the researcher wants to diagnose a situation and attempts to interpret certain phenomenon. They maintain that this approach enables the researcher to gain particular insights and clarify business problems, and subsequently develop new concepts of theoretical perspectives about the phenomenon. "It often has the aim of trying to explain and describe the phenomena from the participant's point of view" (Leedy & Ormrod, 2001, p101). Mikes and Kaplan (2013) found that large statistical studies about apparent ERM practices cannot capture the essence of risk management due to the fact that an emerging body of field studies show an interesting variety of risk-management practices, deployed at different levels, for different purposes, by different staff groups in different organisations.

An inductive approach was followed for this research where the researcher sought to conduct and develop theory from the explanations that arose. Saunders and Lewis (2012) explain the inductive approach as an approach used where the researcher begins with specific observations and measures, observing patterns and repeated occurrences of phenomena and formulate some speculative hypotheses which can be investigated.

The qualitative research strategy of in-depth interviews was used for this research, with archival research to supplement in-depth interviews.

The two strategies are explained below:

- *In-depth interviews:* According to Qu and Dumay (2011), this kind of interview strategy provides a useful way for researchers to learn about the world of others. Myers (2013, p.5) notes “qualitative researchers contend that it is virtually impossible to understand why or how something happened in an organisation without talking to people about it”. This method of conducting in-depth expert interviews was selected to obtain data, as interviews are well suited to exploratory studies using qualitative methods (Saunders & Lewis, 2012).
- *Archival research:* This strategy analyses administrative records and documents as a source of data. While this strategy is generally used as the principal source of data (Saunders & Lewis, 2012), for this research, it will play a supporting role to the in-depth interviews by way of triangulation.

Due to time constraints for this research, a cross-sectional research design was used. Data was collected from the participants at only one period in time – a ‘snapshot’, as described by Saunders and Lewis (2012). If time was not a constraint, a longitudinal research would be preferable due to its ability to study change and development over time. Saunders and Lewis (2012) further suggest that a longitudinal element may be introduced in a cross-sectional research through the use of secondary data sources produced by longitudinal surveys that are available on the internet or in company records.

4.2 Population

While it can be said that every organisation that is running some form of business is exposed to risk and therefore may be the target population, this study aims to understand the phenomena within the mining industry context. The target population for this study was all mining businesses that operate in South Africa and are key players in the global economy. However, it was difficult to obtain a full list of the population as some of the mining companies may have adopted some form of risk management framework and some may not have. Arena et al. (2011) have found that ERM is hard to study because companies are not mandated to disclose their ERM processes. Even companies with some ERM disclosures may not fully reveal their stage of ERM implementation, therefore the sampling frame is not fully known.

4.3 Sampling method

4.3.1 Sampling technique and size

Due to the qualitative nature of the research, as well as the fact that the researcher did not have a complete list of the entire population, a non-probability sampling technique was used (Saunders & Lewis, 2012). Qualitative samples most frequently tend to be purposive, rather than random, which requires the researcher to use his/her judgement to select who would be the best sample respondent to answer the research question (Saunders & Lewis, 2012). A non-probabilistic, purposive sampling approach was used. The researcher wanted to interview participants in companies that have some form of Enterprise risk management implemented and who would be appropriate to provide insights for the research. After initial interviews with risk management practitioners in the industry who confirmed the existence of formalised enterprise risk management in mining organisations, a sample of eight mining companies was therefore selected according to the following criteria:

- Must have implemented ERM for more than two years.
- Include an internal control statement in their annual report. These companies are expected to have more developed risk management and internal control systems, given that they formally report on it.
- Have risk and internal audit functions (separate or combined) with head(s).
- Must be a high reliability organisation (Mikes & Kaplan, 2013) - companies that have no choice but to function reliably. If reliability is compromised, it can cost the company not only financial and asset damage, but human lives as well.
- Have mining operations in South Africa.

The secondary sampling unit was the interviewees in the companies selected. The aim of the qualitative research as outlined by Cohen, Manion & Morrison (2000) was to obtain breadth in information and interviewing more than one person from each company allows for this. However, it was not possible to do so for all the companies. The interviewer was able to interview more than one person in three companies, resulting in 12 interviews across eight companies largely because some of the roles incorporated both internal audit and risk function in one oversight. Another reason was the availability of potential interviewees. However, this still enabled a level of breadth of information to be obtained with the participants emphasising different themes and in some instances, offering contrasting views, and this added to the depth of the interviews. The sample size was deemed to be sufficient based on a benchmark of six

to twelve interviews being the ideal sample size in a qualitative research to enable development of meaningful themes and useful interpretations (Guest, Bunce, & Johnson, 2006).

4.4 Unit of analysis

Blumberg, Cooper, and Schindler (2008) distinguished between five different units of analysis that are common in designing research. These are individuals; organisations; divisions; departments and general groups. This research focused on an organisation as a unit of analysis. It is the phenomena of enterprise risk management and internal control within organisations that this research sought to better understand.

4.5 Method of data collection

4.5.1 Information gathering process

The data for this study was collected using semi-structured interviews with company management of the identified organisations as well as archival research where data sources such as company records and documents were analysed. Such documents included the organisation's enterprise risk management frameworks and risk reports. Management included the executives and managers responsible for risk management and assurance of internal controls. These included Chief Risk Officers or equivalents and Internal Audit Managers.

4.5.2 Research instrument

Saunders and Lewis (2012, p.151) define a semi-structured interview as “ a method of data collection in which the interviewer asks about a set of themes using some predetermined questions, but varies the order in which the themes are covered and questions asked”. This type of interview enables the interviewer to probe with a view to elucidating any vague responses, or to request elaboration when incomplete responses are provided. This level of freedom makes semi-structured interviews particularly applicable to the nature of this research study.

The length of interviews varied between 40 and 90 minutes and were conducted at the interviewees' offices. Some respondents were straight to the point while others provided long responses and others spoke of the history of their risk management journey. Nine out of the twelve interviews were recorded with a voice recorder, and the recordings were later transcribed independently into written documents which the

researcher validated against the recordings for accuracy and completeness. The researcher started recording the interviews after the introductions were done and the purpose of the study was explained, together with signing of the consent letter (see Appendix 2 for the consent letter). For the other three interviews, the researcher made notes, which she transcribed verbatim immediately after the interview while she could still remember, because the interviewees were not comfortable being recorded.

Some paraphrasing, summarising and clarifying techniques were used that allowed the researcher to test her own understanding and to sharpen the focus of vague comments. The phenomena the researcher investigated involved the interviewees' perspectives, their thinking, experiences and decision-making with their specific contexts. Guion (2006) outlines several crucial characteristics of in-depth interviews and the researcher adhered to the guidelines as follows:

- The format of the interview was semi-structured with some pre-planned questions, while allowing for a natural free flow of conversation and questions.
- Questions were open-ended, allowing participants to expand on the topic and not answer by simply saying yes or no.
- The interviewer sought understanding and interpretation of what was heard. The interviewer searched for a deeper understanding and clarity from the participants throughout the interview.
- The researcher recorded responses with an audiotape and a note pad.

An interview guide was prepared (refer to Appendix 3 for detailed interview guide), based on the themes that emerged from Chapter 2 and the research questions developed in Chapter 3. It is exploratory and thus consistent with the semi-structured interview method. Series of questions were explored using following themes:

- The contingency variables defining the context of the company
- The extent to which companies have adopted ERM as a business imperative and why they adopted it. The extent of adoption is evaluated using the ERM maturity elements outlined in the literature review.
- How the adopted ERM approach has enhanced the internal control of the company
- The key factors critical in ensuring that the ERM adopted does enhance the internal control system.

Where new themes emerged, the interview guide was adjusted accordingly to allow for further exploration of the new themes.

4.5.3 Cautions on potential bias arising from interviews

Qu and Dumay (2011) caution that, although this type of research offers great benefits for qualitative researchers, there is a risk of simplifying and idealising the interview situation, based on the assumption that the interviewees are capable and moral truth tellers acting in the service of science and producing the data needed to reveal their experiences and/or the facts of the organisation that is being studied. This was managed by applying a localist perspective to gain insights into the interview method. This means, in following a localist perspective, the eventual aim was for interviewer and interviewee to become equals, with both of them being involved in the production of situated accounts through multifaceted interpersonal interaction. This differs drastically from neopositivists, who treat interviewees as truth-tellers, and romanticists, who are empathetic listeners who explore the inner worlds of the interviewees (Qu & Dumay, 2011).

Podsakoff, MacKenzie, Lee, and Podsakoff (2003) also caution against common method bias as a potential problem in behavioural research. They explain that common method variance is variance that is attributable to the measurement method rather than to the constructs the measures represent. They found that protecting respondent's anonymity and reducing evaluation apprehension are some of the procedures that researchers can use to reduce method biases. The researcher assured participants that there were no right or wrong answers and that they should answer questions as honestly as possible. These procedures should reduce participants' evaluation apprehension and make them less likely to edit their responses to be more socially desirable, lenient, acquiescent, and consistent with how they think the researcher wants them to respond.

Another way the researcher reduced method biases was through the careful construction of the interview items themselves. Podsakoff et al. (2003) found that the most common problems in the comprehension stage of the response process is item ambiguity and cautions researchers to (1) define ambiguous or unfamiliar terms; (2) avoid vague concepts and provide examples when such concepts must be used; (3) keep questions simple, specific, and concise; (4) collapse questions relating to more than one possibility into simpler, more focused questions; and (5) avoid complicated grammar. These were taken into consideration when constructing interview questions.

Another major cause of common method bias is obtaining the measures of both predictor and criterion variables from the same source. One way of controlling for it is to collect the measures of these variables from different sources, as was the case with this research. Measures of ERM implementation were obtained from Chief Risk Officer (CRO); measures of internal control implementation from the board and CRO, while measures of internal control assurance were obtained from both internal audit and CRO.

Saunders and Lewis (2012) also caution against the validity and reliability of data due to common interviewer error. This type of error occurs when the interviewer is not able to write fast enough to record the answers verbatim, resulting in exclusion of important information. In order to address this potential source of error, the researcher utilised a tape recorder (with consent from the interviewees/participants) which allowed the researcher to later replay the interview and transcribe the content at her own pace. However, as noted above, there were three instances where the interviewers were not comfortable being recorded. In these cases, the interviewer made notes as the interview progressed and transcribed the responses immediately after the interview. This does not however eliminate in totality the risk of the interviewer not recording these hand-written responses correctly. This may also lead to the risk of selective perception when the interviewer is recalling and writing the responses after the interviews.

4.6 Pilot-testing

A pilot study was conducted where the interviewer was able to check that the questions prepared were likely to be understood and would provide the data that was needed to answer the research questions. Saunders and Lewis (2012) recommend that researchers need to pilot-test their interviews with a small number of people who are like those who will be participating in the research. The researcher pilot-tested the interview with the subject matter expert in the field of risk management and an internal control assurance practitioner.

4.7 Data analysis approach

Given that the data being collected was qualitative in nature, inductive reasoning was extensively used during the analysis and interpretation of the data. Leedy and Ormrod

(2001) point out that qualitative researchers often discover certain findings and then draw inferences on the larger phenomena and this is called inductive reasoning. The information obtained through in-depth interviews was analysed employing the thematic analysis technique to search for certain themes or patterns across an entire data. For each of the interviews, the main themes emanating from participants were categorised and tabulated around the research questions and themes from the literature review. The process involved the following, as described by Myers (2013), and O'Connor and Gibson (2003):

- The researcher read the transcripts of the interview and the provided documentation.
- To organise the data from the transcripts, the researcher went back to the interview guide to identify and differentiate between the questions the research is attempting to answer and those that were included in the interview guide as important, but not essential. The researcher was cognisant of the fact that the amount of data generated by one interview could answer quite a number of questions and one could as a result spend the rest of one's life trying to analyse all the information (O'Connor & Gibson, 2003). This is why it was important for the researcher to go back to the original research questions.
- The researcher then systematically coded every paragraph in which the different themes of the research questions were discussed.
- For each transcript, the coded sections were copied into an interviewee-based themed matrix. Each interviewee-based themed matrix ended with a summary narrative. This helped to display data in a compressed and ordered form. Similarly, relevant documentation was coded and narrated with the related transcript. This method of organising and displaying data allowed the researcher to look for responses to each topic and specific question individually and it made it easier to pick out concepts and themes.
- The researcher picked out words and ideas that kept coming up and organised them into categories or codes.
- Each category/theme became a basket into which segments of text were placed
- The researcher carefully searched for negative instances of the patterns that did not fit into the patterns and themes of the data and incorporated them into the results.

- There were unexpected findings during interviews where participants seemed to be going in an unexpected or new direction and the interviewer followed up when these instances occurred. O'Connor and Gibson (2003) refer to these as “rich points” which are often valuable. For example, the issue of “bottom-up approach” to risk management became apparent as the interviewers kept mentioning it and the researcher then probed into it.
- Throughout the process, the researcher frequently compared thematic matrices to ensure analytical consistency.

Key commonalities and some differentials were identified during this analysis process which will be explained in the next chapter.

4.8 Validity and Reliability

Any research study should seek to ensure that its findings are both valid and reliable. Saunders and Lewis (2012) use the term ‘validity’ in relation to the credibility of research findings and conclusions while ‘reliability’ is concerned with the extent to which data collection methods used and analysis procedures can be repeated with the same results. This was achieved in this study through triangulation, for instance by also having applied archival research data sources and pilot interviews with subject matter experts in addition to the multiple interviews with multiple respondents. A chain of evidence was established through explicit links among the questions asked, the data collected and the conclusions drawn. Furthermore the potential bias that could arise from interviews was addressed by the researcher as explained above in section 4.5.3. Incorporating these into the research increased its validity and reliability.

4.9 Confidentiality and Anonymity

In order to maintain anonymity of the companies and the interviewees throughout the research process, the writing of this dissertation, the digital audio recordings of the interviews and the transcriptions thereof are kept confidential. Confidentiality was ensured by restricting access to the data to as few people as possible and these included the supervisor of the research and the GIBS recommended transcriber and editor. The names of the companies and the interviewees are not named in this report. However, there is possibility that the reader of this report might be able to guess the identity of the company.

4.10 Research Limitations

It is important to note that while qualitative findings can be replicated, and sometimes be generalised to theory (Yin, 2003), they cannot be inferred across the entire population given the small sample size. Furthermore, due to the fact that the sample was drawn from a similar industry, findings cannot be extrapolated to other different industries. Saunders & Lewis (2012) warned that for this reason, the research should heed drawing definitive conclusions from the findings. Nonetheless, the research findings still provide useful insights into how ERM enhances the internal control environment of an organisation.

Due to time constraints for this research, data was collected from the participants at only one period in time. If time was not a constraint, a longitudinal research would be preferable due to its ability to study change and development over time. This might provide some insight into the way forward for the mining industry in South Africa as it seeks to manage the onslaught of more complex and volume of risks facing the mining industry due to the changing economic and business landscape brought about by globalization, the geopolitical environment in which these companies operate and the inherently dynamic nature of the context of this industry. In order to gain better understanding of the constructs being explored, there is a risk of interviewer bias where the interviewer may have asked leading questions that may have influenced the respondents' answers.

CHAPTER 5: RESULTS

5.1 Introduction

The previous chapter explained the methodology used to explore the research questions outlined in Chapter 3. The results are therefore presented in alignment with these research questions, thus informing the layout of this chapter. All results and findings were summarised for each research question and were directly correlated with the questions posed in the data collection tool. The chapter commences with a brief description of the sample. Thereafter the main themes and observations are discussed under the relevant research question. Then, the researcher expands on each of the major sub-themes per research question. The chapter thereafter concludes with additional research findings as well as a summary of key findings, which will be further interpreted in Chapter 6.

5.2 Sample description and response rate

The data for this study was collected using semi-structured interviews with identified key players in the mining industry. The participants were identified because of their in-depth understanding of the phenomenon under investigation. The research participants' perspective and the meanings they derive from situations were also sought with the aim of understanding the operationalization of risk management within different mining organisations and how that has impacted their internal control systems. Further data sources such as the organisation's enterprise risk management frameworks, risk reports and annual financial reports were used to validate the responses received from the interviewees.

Eight mining organisations were contacted by means of phone calls and emails with a cover letter explaining the nature and scope of the research. Cover letters detailing the nature of the research were sent to the Chief Risk Officers (CROs) or the equivalent, who in turn, referred the researcher to the different heads of internal audit in instances where, the function was a separate unit from the risk function. One of the research respondents was not a risk or assurance specialist, rather the Chairperson of a board of one of the mining organisations. The respondent's inclusion was subsequent to the challenges experienced in obtaining an interview with the individual responsible for risk coordination in their organisation. Due to the respondent's role and duty as a Chairperson, the individual was well suited for this research because of their in-depth

understanding of the phenomena under investigation from a board-level perspective. Interviews were scheduled directly with the individuals direct. This resulted in twelve face-to-face interviews being conducted across eight organisations. Thus, some organisations had more than one representative interviewed. A semi-structured interview was the selected method of data collection, as elaborated in chapter 4. This research method enabled the researcher the flexibility to probe deeper into the subject matter in order to uncover new insights and valuable knowledge. It is important to note that not all of the 12 interviewees answered all of the interview questions as consistently.

As explained in Chapter 4, nine out of twelve interviews were recorded and transcribed while the other three interviews were not recorded, but thick description notes were taken which the researcher transcribed immediately after the interview whilst everything was still fresh in the mind. The average length of the recorded transcripts was 15 pages while the notes taken by the researcher resulted in transcripts of an average of 5 pages each. The sample obtained and the input received has enabled each of the research questions to be explored and has therefore satisfied the research objectives. The researcher asserts that the response selection process was adequately applied which resulted in a satisfactory respondent list. Table 2 below provides a summary list of interviewees per company.

Table 2: Summary description of interviewees per company

Company Reference	Number of Interviewees	Position of Interviewees
Company 1	2	<ul style="list-style-type: none"> • Head of Risk and Assurance • Senior Risk Manager
Company 2	2	<ul style="list-style-type: none"> • Senior Vice President: Group Risk • Senior Vice President: Group Internal Audit
Company 3	1	<ul style="list-style-type: none"> • Chairperson of the Board
Company 4	3	<ul style="list-style-type: none"> • Chief Risk Officer • Group Manager Risk and Compliance • Senior Project Risk Specialist
Company 5	1	<ul style="list-style-type: none"> • Chief Risk Officer
Company 6	1	<ul style="list-style-type: none"> • Chief Risk Officer
Company 7	1	<ul style="list-style-type: none"> • Sustainable Development Manager
Company 8	1	<ul style="list-style-type: none"> • Risk and Insurance Advisor
Total	12	

For the purposes of confidentiality, the identity of the interviewees has intentionally not been disclosed in the research findings as stipulated in the research methodology in Chapter 4. Confidentiality has been ensured by allocating random respondent numbers, as well as by presenting the research findings in a way that the individuals could not be identified. Through this process, the subsequent quality of the content of the findings has thus not been altered.

5.3 Research Question 1: To what extent have organisations adopted a formal enterprise-wide approach to risk management and why did they adopt it?

The first question sought to provide a basis for discussion around enterprise risk management. In this question, research respondents were asked about their enterprise-wide approach to risk and why this approach was implemented. All research respondents were able to talk directly to this question, and were able to articulate clearly their current approach to risk management and why that approach was adopted. The answers provided were aligned, and respondents spoke of the nature of the mining industry and the different regulatory frameworks that must be met, such as health, safety and environmental standards. Themes that emerged from the interviews when it comes to the organisation's adopted enterprise-wide approach to risk are explained below.

Current approach to risk management

All research respondents indicated that within their line of work there is enterprise-wide risk management that is being undertaken. The mining sector in South Africa is well developed and responses indicate that there is significant development and understanding with regard to risk management within the South African mining industry. The following respondent points out that South African mining organisations are well advanced with regard to enterprise risk management.

“I don't think there are many other countries that does it as well as we do in SA. I am talking risk management more than internal audit. I am not a risk manager so I am not bragging; I am complimenting the risk management people in SA”
(Respondent 5)

In trying to understand the afore-mentioned advancement of ERM, the researcher examined the ERM frameworks of the organisations that were interviewed using the identified characteristics of ERM maturity. Whilst these characteristics are not an exhaustive list, they can, in light of the literature reviewed in Chapter 2, provide a

measure of maturity of ERM, thus by giving an indication of the extent of adoption of ERM.

Results from the interviews reveal that the interviewed organisations' ERM practices are between intermediate and mature levels of maturity. This provided a sound basis to better understand how then the ERM system in place has impacted the internal control system of the organisations. The results are summarised in Table 3 below outlining certain characteristics that were identified. The commentary following the table provides more details on the findings.

Table 3: ERM Maturity of sample organisations

Immature Intermediate Mature



Characteristics of ERM maturity	Companies 1 to 8							
	1	2	3	4	5	6	7	8
Framework that incorporates all of the company's key risks	Green	Green	Green	Green	Green	Green	Green	Green
ERM objectives communicated and tied to KPIs	Red	Red	Red	Red	Green	Yellow	Yellow	Yellow
Strategic focus of risk (Integration of ERM in strategic planning)	Green	Green	Green	Green	Green	Green	Green	Green
Specific risk limits and business boundaries set, i.e. risk appetite of company	Yellow	Red	Green	Yellow	Green	Green	Green	Green
Risk-aware culture	Red	Yellow	Yellow	Red	Yellow	Yellow	Yellow	Green
Independent ERM function under leadership of CRO	Green	Green	Yellow	Yellow	Green	Green	Yellow	Yellow
Board-level oversight	Green	Green	Green	Green	Green	Green	Green	Green
Dynamically adaptive and proactive ERM process integrated into business processes	Yellow	Green	Yellow	Yellow	Green	Yellow	Yellow	Green
ERM dashboard technology and reporting capability integrating key risk metrics	Yellow	Yellow	Yellow	Yellow	Green	Yellow	Yellow	Yellow

All the organisations included in the study are more mature in the ERM maturity characteristics that talk to the governance aspects of ERM such as board-level oversight of ERM, the integration of ERM in strategic planning, existence of an independent ERM function under leadership of CRO, and having formal framework that

incorporates all of the organisation's key risks with specific risk appetite. Two respondents interestingly provided a different dimension to the issue of setting risk appetite. They acknowledge that while setting the risk appetite helps to define the level of risk the organisation is prepared to operate within, they have not been able to do it properly as defining risk appetite and tolerance is a challenge, particularly in an industry that has so many different types of risks.

"But what we haven't yet done properly is to properly define risk appetite and tolerance, that is the challenge, I need to focus on that now. In the banking world it might be a bit easier but when you have so many different types of risk it is very difficult to actually quantify in my opinion – but that is my next challenge (Respondent 12)

"It is a difficult thing to set, how do you set a tolerance level on safety? I am not going to budget to hurt anyone. On environmental how do you budget, and then how do you translate that to money?...I won't sign anything off ever, that says 'okay we had ten fatalities last year, if we have six this year we are good.' You are not, you have killed six people, and that is some of the difficulties around tolerance, to say 'okay does that mean we now need to close this mine because we had two fatalities?' So it is very difficult. So the tolerance is something that I don't think people understand and it is incredibly difficult and it can't be a one size fits all, it is very fluent" (AngoGoldInt)

All respondents have a formal ERM function. Depending on the organisation, the ERM function is either a separate function or it is still integrated with other functions such as internal audit or finance. Furthermore, a hybrid structure of ERM function is employed. This means that the ERM function combines the advantages of centralised and decentralised structures to enable adequate and timely reporting of risks. In this structure, the different business functions perform their own risk management activities such as identification and analysis of risks and implementation of control measures supported and coordinated by a central risk management department.

Risk management is integrated into operational business processes in each business department through a long history of silo risk management. The respondents explained that most of the department and mine managers have an overview of their risks. However, on specific processes such as communication of risk objectives and

performance measurement, varied maturity levels ranging from immature to mature are observed. Particularly for the performance measurement, the majority of respondents acknowledged that risk management is tied to Executives KPIs and that it has not filtered down through the organisation. Certain aspects of risk management are included but the little that is included is more detailed around safety risk management. The overall risk culture also provided these varied maturity levels. This demonstrates that organisations have not fully integrated ERM with other business processes and with the culture of the organisation.

What is interesting to note is that while specific risk management tools are being used to support risk management, majority of the respondents highlighted the challenges of using different systems that do not interface with each other at operational and corporate levels. This makes the ERM process much more complex as explained by Respondent 1 in the next page.

In the responses provided below, there is recognition that there is more that needs to be done when it comes to ERM. The respondent acknowledges that there is a concerted effort being made towards ERM. Despite this, as highlighted in the section below, risk management can take a narrow focus, which can prove detrimental to the maturity of ERM with organisation.

“Enterprise wide risk management, I think companies are starting to get there. There are very few companies that I think are even 70% where they should be, I think we are at about 65%, and I think we are fairly mature compared to others because you find that unfortunately with risk management, very often it is a very narrowly driven process, from a corporate head office, where a couple of people sit and sort of advice the rest; then you get to a site, a business unit, and they either don't know about it or it is stuff that gets given to them by corporate, and it doesn't come from that side as well. So I think that is the first issue” (Respondent 5)

More lately, greater emphasis has been placed on businesses to reevaluate how they deal with risk management. Risk management has moved beyond the traditional practice whereby risk was narrowly-focused and silo-based, particularly around safety and health risk in the mining sector. Mining organisations have appreciated that ERM provides them with a better mechanism to internalise risk management. However, the challenge still lies with the maturity of the ERM process for the organisation to realise the full benefit of ERM on the internal control system.

Challenges with bottom-up approach to risk management

While the respondents acknowledge that the understanding of enterprise risk management in mining has developed, three respondents provided new additional insights that when it comes to ERM, they perform the top-down risk management very well, however they are still experiencing challenges with the bottom-up approach, which speaks to ERM maturity measures such as risk communication and performance measurement and the organisational risk culture which are varied between immature, intermediate and more mature levels.

“There is no enterprise ‘anything’ at the mine; it is safety risk, safety risk, health risk, health risk and environmental risk - that’s it. So it is very safety, safety, health, health – you know. So that is their risk world, there is no enterprise health risk. But as you go into the mine manager level there will be more of a mine-wide risk mentality; when you come to corporate there will be an enterprise risk mentality...they don’t understand what we are looking for in terms of enterprise risks; their risk register is writing down the top five safety risks, or what he has to. So it is very, very difficult. So the top down risk management is very easy for us; you go chat to the CEO, you chat to CFO, you chat to Audit Committee Board, EXCO – they understand risk – to get the top level strategic organisational, external type risks you can do very easily. You can also get the middle layer of operational risks fairly easily, but if you want to get mine-specific, process-specific at the mine level, that is very difficult. So the bottom up risks, the bottom up risk process is a challenge.” (Respondent 10)

“This is something you will find we have sort of ad hoc meetings with my colleagues at [other mines], so when I say this I speak on behalf of the mining industry: what happens is at this level here you have certain systems, we call them Isometric or pivot systems, it is like a SAP or JDE, it is systems which are specifically designed for those processes, and then from these level upwards we use what we call CURA, which is risk software which you should know, so yes, this is why I explained to you: at this level, or when we do those risk assessments key or major risks that is coming out of your safety health environmental processes, and that is my biggest challenge, is how do I connect this process, this safety health environmental operational risks to the more corporate strategic risks. And the answer is there is a disconnect and that is where my work, when I facilitate these risk workshops, to ask every single time, I ask, and that is why I need to read operational reports, I attend operational

committee meetings, I sit down with the GMs, with other managers, to make sure that I understand what are the risks in that environment so we can highlight them in the strategic level or at the process level. That is the challenge we face and that is what you will find at [other mines] – we all have the same problem... that is the problem we face in a mining industry, or challenge we face – not problem – it is a challenge.” (Respondent 1)

“Yes, But we are still battling with bottom up risks. I think we are doing well in terms of top-down risks.” (Respondent 6)

Mining industry has a developed regulatory framework which the mining organisations have to comply with

With the economic crisis 2008-9, many businesses have come under scrutiny for the way they function. Both developed and developing countries are under pressure to move away from compliance approaches that are only focused on results. The minerals resource sector in South Africa is an important mechanism used to drive South Africa’s development trajectory. It is also important to note that this is one of the oldest economic sectors in the country and houses some of the big names internationally when it comes to the minerals industry. Thus, it has a well-developed regulatory framework which mining organisations have to comply with. The responses provided by the research participants provide an indication that there is greater awareness regarding the existing regulatory frameworks in place, which they have to comply with. Unfortunately, most of the respondents indicated that in most instances, the main practice is based on meeting those standards.

Mining can be a dangerous exercise, and the legislative framework in place is there to mitigate some of these safety, health and environmental challenges that come with mining. The responses below provide a good indication of this compliance based approach. All respondents are aware of the statutory framework for operating a mine, and due to regular mine audits, which are undertaken by the department of Health, Department of Water and Department of Environmental Affairs, there is greater awareness of the need to comply.

“...and then I guess another one of the big issues is all the legislative requirements that you have to comply with and make sure you are legally compliant, especially in the SA context, you know, not upsetting the Department of Mineral Resources, your safety issues are extremely important.

If you are in contravention they will close you down, they will stop production until you get your house in order (Respondent 9)

“Okay, I think risk is still probably being seen as a compliance function and therefore doesn’t have technical skills.” (Respondent 12)

“The last component is all the governance, around risk management. I mean risk management is sometimes seen as just governance. And it is not just governance.” (Respondent 1)

The responses below provide a good illustration of the regulatory requirement. There are few Government departments that the mining industry has to comply with regarding risk management, and in most instances, it outside the mine’s core function, such as environmental issues, but is equally important to their sustainability.

“We have our external guys...department of minerals, department of water affairs-anybody that is independent from the operational or independent from the company. So that is how I usually explain this to guys so they see where we as risk management fit in” (Respondent 1)

“So what we have tried to do is to say that there are a lot of codes of good practice and regulatory requirements out there with regard to risk management, and sometimes companies tend to implement risk management because they want to comply to those codes of good practice, or they want to comply with those regulatory requirements” (Respondent 8)

Respondent 11 mentioned the benefit of ERM that it simplifies the compliance process such as OHSAS, ISO etc. in that it reduces the external tier’s assurance activities that they used to do for compliance. Each individual department used to be charged separately for these separate compliance exercises.

The mining industry in South Africa has a long and rich history that dates back as far as the discovery of diamonds in Kimberly and the discovery of gold in Gauteng. This sector continues to employ a significant amount of people in the labour market. The established and regulated industry, through various government bodies such as the Department of Minerals, Department of Health, Department of Labour and Department of Water Affairs is also an indication of the development of the regulatory framework.

Enterprise Risk Management viewed as a business imperative

Research participants acknowledge that there has been a significant shift in the way business views risk management. Even if there are compliance requirements due to the regulatory environment that the mining organisations operate in, the focus of risk management is now changing. ERM is seen as an instrument that can help organisations to manage their risks better.

Respondent 8 explained that their organisation unpacked the various codes of good practice, ISO standards, compliance requirements from the JSE's side and general Companies Act's side to realise that what sits at the heart of risk management is a good, well-defined management system that will enable achievement of strategic objectives:

“So it is about management, it is about good management, it is not about ticking those boxes, and if you make that shift that it should be a business tool, business should buy into it, they should believe that there is value to it, that you can truly benefit the organisation; because then you can tick the boxes but you would have achieved so much more, because you would have achieved what sits at the heart of good risk management, and that is achieving your strategic objectives.” (Respondent 8)

Similar views were shared by other the respondents:

“...there was a new focus on risk management, and that meant the restructuring of risk, away from internal audit, and risk was then put with business strategy with the goal of risk management being to properly inform strategy, which helped to break down silos. The focus is now not only per discipline, it is across all of the disciplines across the group.” (Respondent 12)

“In so far as ERM is concerned, I mean when the first King report came out, [our organisation] tried to implement ERM and it was really just filling out spreadsheets every six months for the purposes of reporting. Then obviously we had the economic crisis in 2008, and obviously some part of it moving in to 2009, and the financial director put a lot of emphasis on getting ERM right.” (Respondent 9)

A need for more integrated view of risk

The participants pointed out the need for a more integrated view of risk. Their responses indicate that ERM is no longer about just ticking the boxes for compliance or

for corporate governance requirement purposes, ERM is seen as a business tool that organisations can base decisions on.

“There was cost pressure in the organisation and people no longer wanted to just tick boxes, any function needed to prove that it will add value and contribute to business efficiency, and we couldn’t afford anymore to have a silo-based approach or approach to risk management” (Respondent 8)

Traditionally we have had silo-based risk with focus on safety and health risks...we wanted integration of risk. We wanted to combine internal view and external view to get one view of risk. We started looking at community risk, health, safety and environmental risks but at an organisational level.” (Respondent 4)

“...before that IM or IT had their own risk management methodology, finance had their own thing going on, safety health and environment had their own methodology. So we decided that if we really wanted to get the value out, we need to standardize – because if you want to use it [ERM] as a management tool, if you want to be able to base decisions on it, it needs to speak to one another.” (Respondent 8)

5.4 Research Question 2: How does ERM enhance an organisation’s internal control system?

ERM brings greater improvement to internal control, and more importantly, it is a strategic tool that can also influence how the business functions in the future. The aim of this question is to also identify those organisations that are operationalizing ERM, and getting to elaborate on the impact that this has had on their internal control system. With this question, respondents were reflecting on how ERM enhances their organisation’s internal control system. There is a strong emphasis placed on identifying the risks that can be controlled. This question was also aimed at bringing out the advantages that an enterprise-wide control system brings to the organisation, and trying to draw a distinction between the traditional practices whereby in most instances they worked in silos.

Understanding ERM as a key component of the business strategy

Research participants acknowledge that there has been a significant shift in the way business views risk management. The argument has moved beyond looking at the

financial indicators as the only key component to business success. Most of the research participants have indicated that ERM with its strategic focus has enhanced their internal control systems:

“So it is all inter-connected. And we said at the start, people being very concerned about the financial risk and we are only looking at that, that is only 10% of the picture, the sustainability, the health, the safety issue can take you out of business probably quicker than the financial issue. So it is really getting the enterprise-wide view and doing it properly, and then assuring it enterprise wide as well” (Respondent 5)

“...if you don't have proper controls you are very unlikely to achieve your objectives and that is the one area of risk management that a lot of people don't fully grasp I don't think, is that your risk management process must be defined, or your risks, in the context of your objectives because the reason that you exist is to achieve certain things. Now what are all the things that are going to prevent you from achieving that – those are your risks – and then what are you doing about it is your controls. So if you are not controlling your risks you are not going to achieve your objectives and that to me is the fundamental objective of risk management and having a proper control environment.”(Respondent 9)

“Yes, our controls have more meaning as to which risks they are controlling and for which business objective they are helping achieve” (Respondent 11)

Respondent 7 had a different view about risk management's shift towards a more strategic and integrated focus. The respondent is of the view that risk management has always consisted of the strategic focus as explained below:

“Strategic component to your risk management approach of risk has always been here, it has also been here for 100 years, it is just that they started giving it new names, and all sorts of things, because when I started in the mining industry 30 years ago we were doing this, it was just called something else you know; it wasn't as well branded” (Respondent 7)

ERM enhances internal control system through improved focus on the right risks

Majority of the respondents concur that ERM impacts positively on the internal control system and this is seen from some of the responses below.

“So how has risk management improved our internal controls? I think it creates the focus because we have now identified this risk, we have shown the control effectiveness is not good, so now there is the focus, everybody is aware of it, it is not something that somebody forgets about, you are reminded about it every quarter, and then because we have this other process where we have the actions, once that control effectiveness is not considered to be good, or if it is below good, there are actions that need to take place, and those usually result in your control environment improving” (Respondent 1)

“Sustainability in a mining company is crucial; communities, environmental, safety, health – those are massive issues and there is big overlap between those issues and HR, between those issues and security, between those issues and finance even – technical finance and stuff like that. So the moment you start breaking down those silos I think that is where ERM kicks in and helps improve the controls through the process” (Respondent 5)

“So yes, it has improved the focus on identifying the right risks and the ultimate goal is to make sure that once we have identified all of the risks, that the risks are properly controlled from a preventative point of view as well as a mitigatory point of view. So it has given structure to processes, including that of internal audit” (Respondent 12).

“[Internal controls] are based on sound risk management process that takes into account the context of our business” (Respondent 9)

Furthermore, with regard to the design of internal controls, majority of the respondents acknowledged that prior to ERM, their controls were “badly” designed.

“Very badly” (Respondent 8)

“So you may sign off on all the controls but actually that risk may not be properly controlled. So for example a particular type of risk for us... we mapped it recently and we had something like in excess of 109 different controls, which you would think would prove this risk was properly controlled, but actually 90% of those are administrative, and therefore bits of paper mostly, and some of the root causes of that risk were not properly controlled at all, so that is something I have cautioned needs to be done in any enterprise, is to make sure that the risks are properly understood and properly controlled, before you go and actually audit the risk, the controls.” (Respondent 12)

Respondent 7 was the only one with contrasting views about ERM and its impact on internal control.

“So the important thing is that we see internal controls as an established process to mitigate certain risks, quite a few of them, especially the financial risks and the ethical and governance risks, and that is how we see it”
(Respondent 7)

In attempting to clarify Respondent 7's position, the interviewer attempted to paraphrase the response from the respondent and re-phrase the question and the response did not bear much clarity on the question of whether ERM enhances the internal control.

“It is basically a mitigating strategy. When you are looking at enterprise risk management it is a process, you are looking at what is the risk. Then for every risk, it doesn't matter what the risk is, you have got many, many control measures, lots of things you are doing on a daily basis, that lots of people are doing to try and mitigate the risk, and those are what we call current control measures. Now SOX is a current control measure for many, many different risks, especially the financial risks, and that is how we see it. And in spite of those control measures you still have a level of risk, things can still go wrong, that is why you have further mitigating actions, that is why you think up these extra things you need to do, to mitigate the risk even further. So the control measures that are already in place, and SOX is a control measure for the breach of the code of ethics risk, for a financial risk, for a lot of things. So is internal audit, the audit is a control measure. And then like I say what we do on a six monthly basis is we assess this thing, we have a look at the risk, is it still a risk, ja, look at the control measures and the risk ranking, the level of the risk and we look at what we said we were going to do last time, are we still doing it”
(Respondent 7)

Internal audit as an important aspect of internal control, driven by ERM

Prominently, research participants indicated that internal audit is an important component of internal control in the business and that through ERM, the value provided by internal audit is much more focused and ties to the risks pertinent to the achievement of the organisation's strategic objectives.

"I think you know the way we audit now is completely different, it is risk-based audit. We actually do I think more non-financial assurance now than financial! So we are auditing more other internal controls than financial internal controls. I think the focus totally changed. There is a bigger understanding of the operations that we need to audit, those controls that manage very high risk, that we say are very effective. So increasingly that message is getting through."
[Respondent 8]

"...but again the emphasis was on process. So you would take an organisation and you would say 'okay these are all the processes that exist within the organisation' and then you would go and audit the controls in those processes. Now it is determined by what are your key risks. And do you have enough to support the mitigation of those risks, as opposed to just mapping out a process and then auditing the process and you never really know how the process impacts your objectives. And sometimes it will, obviously a lot of times it will because typically you design processes to achieve objectives, subconsciously. But now at least you know that your focus is on these are the really important areas that are going to destroy your profits or your triple bottom line. Therefore ERM has also helped in how we review the effectiveness of the controls"
(Respondent 9)

"You cannot do combined assurance, or even proper assurance if ERM isn't in place and working. So only when risk got this process to a point where it started to mature, and that was about three or four years ago, we could start implementing all of this, and that is why the relationship is so close between us [internal audit] and [risk], although we are totally different departments."
(Respondent 5).

"The bulk of our audit plan is guided by the enterprise risk" (Respondent 7)

"So if I had to look at that, we can see a definite decline in the number of ratings in the areas, we have seen a heightened awareness from management on how those controls impact their risk, to the point where internal audit have been invited to the weekly EXCO meetings, to report on risk and assurance. And the impacts of our audit results. We also then have to report on how management have actioned our audit findings, because we are actually showing a direct impact on our audit results on the risks on the organisations."(Respondent 10)

Other measures of internal control improvements

Most of the research participants pointed out the importance of having an integrated risk and control reporting, as an important measure of how well the organisation is managing the internal control, thus managing the risks that threaten achievement of objectives. Various reports were shared with the interviewer. Although the various reports' format differs, all of them contain features that integrate ERM, strategic objectives and internal control.

“Four years ago half those [internal control] boxes would be red, a quarter would be yellow and a quarter would be green in terms of how well the controls were working.... and the last register that I saw was about 60% green, 25% yellow and 15 to 20% red.” (Respondent 2)

Respondent 11 added that they have seen improved motivations for capital budget requirements because it must be to significantly control a major risk exposure. In addition,

“assurance process has improved, we don't need external assurance anymore as our business units would call external parties to review their internal controls. We have shown a Rand value saving” (Respondent 11)

While risk and control ownership at Exco level was highlighted by other respondents as one of the benefits brought about by ERM, three different views about risk and control ownership emerged.

“We have a risk owner and control owner per risk with specific timelines. At Exco level is tied to their KPIs and they take it serious” (Respondent 11)

“The answer should be yes but the extent to which there is proper accountability and consequence management at times is so low in these companies that you have to wonder whether that ownership is really there, because you don't, which is a bigger and bigger issue now, that consequence management, boards are starting to take it more seriously than was the case in the past.” (Respondent 2)

“We are in a bit of a strange cycle now: because management have started... let's put it this way -the more your boss starts asking you about internal audit findings, and the more awareness there is created, you get a very, very fine line between management taking the responsibility to sort things out, and over-

reacting. In some areas we have had extreme over-reaction, where you have got management actually hiring their own little audit teams to go and audit themselves, to make sure that they don't get weak and inefficient reports...so you are going to have that reaction. So sometimes you have over-reaction, where they are auditing themselves six times over before..." (Respondent 10)

Reasons for minimal internal control improvement in other areas

The respondents below provided slightly different views on how ERM has improved the internal control system of their organisation. Respondent 5 seems to believe that ERM has not improved internal control while three other respondents are of the view that the improvements are still immature. They point out some of the issues that need to be addressed in order for ERM to achieve the desired impact on internal control systems.

"Okay, so now your question is has internal controls improved with the ERM, and I guess not really, because I think there was a big misalignment. So what you had in most companies is internal audits did their own bit of risk management to build their audit plan. So they had this risk exercise and they built this audit plan and a lot of it was my knowledge of the company and asking my clients and such and such. And risk management was on the other side or in a lot of companies risk management/internal audit was the same function" (Respondent 5)

"It is looking slightly better but I can't attribute that to ERM per se. At this stage ERM is giving the mine management the understanding of key control – what they need to focus on to ensure there are no "shocks". Avoid shocks and more certainty around achievement of objectives" (Respondent 6)

"Look, we are not yet there in terms of our ERM efforts. we are a bigger operation and silo- controls management still exists in other areas" (Respondent 4)

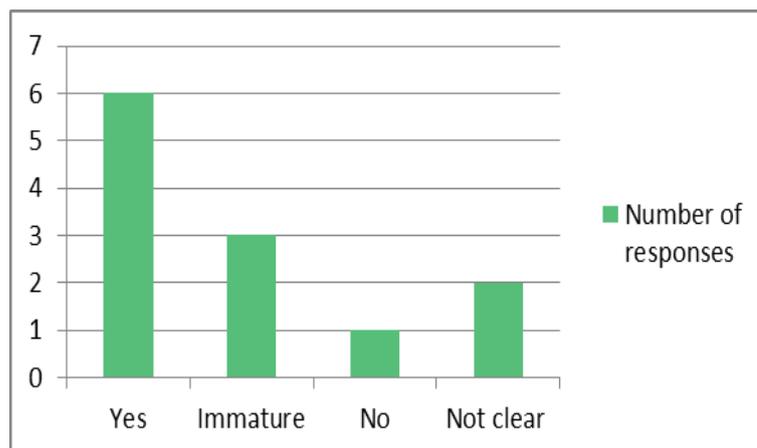
"Look I think for me that is the area that you can't prove exactly, but I think when you have successfully implemented ERM you will have, you should have more consistent results. So hopefully even in bad times you have sufficiently thought about those things so it doesn't impact your bottom line too badly. Now generally we are a disciplined company so it is not that you needed the implementation of risk management to continue to be disciplined, but what the process has brought is a lot of structure, so that we can think about when

things are going wrong are we doing enough about it. So I don't know if I can say that it has improved the performance of the company consistently - I think we need maybe a longer period to test that – but certainly what it has done is highlighted when things are going wrong and are we doing enough to fix those things.” (Respondent 9)

The above responses allude to the issues of alignment of ERM with internal audit as well as the maturity of the ERM process that affect how well the ERM process can then influence the internal control system.

The overall responses to question two are summarised in Figure 5 below, showing the number of responses received on whether implementing ERM has enhanced internal control systems of the organisations.

Figure 5: Views on whether implementing ERM has enhanced the internal control system



5.5 Research Question 3: What are the key factors that are critical in ensuring that ERM enhances an organisation's internal control system?

This question follows on research question 2 in that it seeks to better understand, more especially from those organisation that have a matured ERM system in place, what the factors are that ensure that ERM enhances an organisation's internal control system. More importantly, this question also draws out from respondents, what they think might be key factors that could affect the success of ERM and its benefits to the control system of the organisation.

The role of leadership is paramount to the advancement and successes of ERM

Implementing a new system within organisations requires buy-in, more especially from top-management. Research participants who work in organisations that are operationalizing ERM indicate that there is a need to get organisational buy-in, and this goes all the way to top-management. Research participants also indicate that there is a need to change the organisation culture if ERM is to become an important component of risk management.

“Getting the buy in from business and the kind of leaders your organisation has is crucial”. (Exxro CRO).

“I realized I needed top level support, and that is not negotiable” (Respondent 12)

“Number two is the credibility of your chief risk officer.” (Respondent 7)

“Leadership is key; your EXCO need to believe in the process and set the example. So if you set up meetings and people don’t arrive, that is really a leadership issue and I certainly think we haven’t got that totally right but I think we certainly have strong leadership in a lot of areas” (Respondent 9)

“Look, if the guy at the top doesn’t show much interest then it is going to fail, it is not going to take off, because you as a risk manager have got no.... you know people have lots of work to do, they don’t have time to sit and listen to your stories so if you don’t have support from the CEO it won’t ever take off because people do what is on their balanced scorecard” (Respondent 7).

“...definitely, you know if something is not driven at the top, it kind of lose some... even if I was there and trying to make sure that the risk management is embedded within the project environment. But without the top being centred, we wouldn’t go far.” (Respondent 3)

Two respondents below went so far as emphasising that the tone at the top alone is not going to achieve results, it is important that that tone drives the behaviour across the organisation.

“Well I mean the tone at the top is critical, is important, without it nothing much happens in most organisations but the tone at the top is a.. it by itself does not make an organisation behave the way it should behave. The ability to translate the messagings that come from the top so that they effectively percolate into the organisation and everybody else can live that culture, is even more

important than the tone that is set at the top... so the more important issue for me, the tone at the top is important, it is a necessary condition but it is not the only driver; the ability to drive it into the organisation and to change the consciousness of each individual employee or stakeholder is more important in my view.” (Respondent 2)

“...I think generally it is more of a push than a pull, so whilst our senior executives say that they really believe in the process and it is important, it is not always evident in the time they allocate to it, and the activities that should sometimes be happening. So I don't think we can say we have arrived in that space, it is like as the [role of respondent] I often felt like I was pushing the process, whereas that wasn't really my job you know; the executives must say 'this is the process and you will follow it' etc...” (Respondent 9)

The maturity levels of ERM within organisations go a long way to seeing the true value of this process.

Research respondents indicated that the true value of ERM is diminished when the level of ERM maturity within an organisation is minimal. As pointed in the above section, there are other key factors such as senior managers and leadership buy-in that are required in order to have the desired impact of ERM on the internal control system, more importantly, there is a need to change the organisational culture.

“So what we are really trying to do now is really make sure, firstly that risk management is at the right level, because if your risk management isn't mature enough you are going to test what you think are the key risks and it is not.” (Respondent 5)

“And I think that is where your question around 'does risk management actually improve the control environment' – it depends very much on the quality and maturity of the risk process. So if you have a very structured process so if you make sure for example when you have your risk reviews that you are reviewing your context properly, because you have a list of risks that typically affect any industry or any business. So they maybe change a bit here and there, but what actually changes is the context, and people are not very good at reviewing the context, to see how it impacts their risks and controls” (Respondent 9)

“Where you implement controls in one area for example in finance usually it will impact something in IT or vice versa. ERM has not yet made it easier for those

kinds of things to be picked up early, before you decide. Maybe there is more of an understanding that needs to happen, plus a collaboration on certain activities within one control but we are not there yet” (Respondent 8)

Within the organisation’s maturity context, the risk culture plays a huge part in how successful organisations are in driving ERM and internal control focus,

“So you need to be able to adapt quickly. The only way you can adapt quickly is if you think proactively all the time, and you know, that is what you want to achieve. So changing that, changing the risk culture is what takes time and we are getting there” (Respondent 8)

“...if I could go back and redo this [number of years] ago, I would have some sort of awareness campaign or change culture program that I would do, to just change the culture of the organisation to show how to do it differently.” (Respondent 1)

A simple risk process is what is required.

“Keep the process simple, it must be appropriate to your risk maturity, mining is pretty unscientific or uncomplicated, we are not high tech unfortunately, so most of the risk management skills are actually quite low based, so you need relatively simple tools”. (Respondent 12).

“Second would be to have something simple, not rocket science, because people don’t want that, you need to be able to explain this to the lowest level employee to understand what is risk management. So at the top, have a simple practical process, and then to show the value.” (Respondent 1)

“You have got to have an ERM process which is simple, and well-understood” (Respondent 7)

Respondent 2 concurs with the above respondents’ view about a simple process that can be understood by everyone. The respondent points out that:

“..you know it really has become so complex to manage enterprise risk because the more you understand and embrace it comprehensively the more complex it makes the operational matrix” (Respondent 2)

“..and so our challenge in a company like [ours] is that the majority of the people in the bottom end of the mining spectrum don’t even have matrix.

Language of communication is “Fanagolo” which we are trying to change...You know, they can barely read and write, they can barely comprehend at the level of complexity of comprehension...But you know your question is enterprise risk question, so to what extent do those people worry about environmental sustainability issues? They don’t. And you have to. Because of the level of education, because of the nature of the work that they are doing, it is easier to communicate with them when you give the line of sight issues” (Respondent 2)

Risk must be viewed within a context:

*“..and in my view a lot of risk management processes haven’t put enough emphasis first of all on understanding changing context and then looking at those controls..are they still appropriate and actually working and effective?”.
(Respondent 9)*

5.6 Other results presenting contextual considerations for ERM

Every organisation has different internal control requirements, circumstances and objectives and ERM application also varies depending on the organisational context. It was therefore necessary to determine such contextual elements in the organisations that were interviewed and take them into consideration when evaluating the findings. The researcher highlights and brings forth the three identified characteristics of size, culture and the industry the organisations operate in since they influence how risk and control systems are applied within organisations.

The results from the interviews are summarised in Table 4

Table 4: Summary of contextual elements that influence ERM and internal control application

Contingency characteristics	Main findings	Responses from interviewees
Size of Organisation	Research participants indicated that the size of the organisation shapes ERM and internal control activities in an organisation. It influenced how extensive and effectively the ERM framework was promulgated within the organisation.	<ul style="list-style-type: none"> - When I first started it was 100000 people, 30 years ago, so we have got a hell of a lot smaller...so it is very easy now, it is much easier – the smaller you are the more control you have. (Respondent 7) - In SA probably 4500 and globally 12000...the small size of our organisation has enabled us to be where we are with risk management. I think it is a lot more agile (Respondent 9) - Yes we are a big operation [60000] so to get the risk message to everyone is a challenge. We are not yet there in terms of ERM (Respondent 6). - ...both the size and the maturity of risk management absolutely shapes ERM. It is not only the size; it is actually the geographical spread of our operations. So it is quite difficult to learn something when you don't speak [country-specific] languages? (Respondent 12)
Industry of Organisation	An industry within which organisations operate has an influence on how ERM is applied within the organisations.	<ul style="list-style-type: none"> - Look to me that question is often an interesting question because by nature of the fact that you have chosen to be in mining immediately exposes you to a lot of risk (Respondent 9) - Most mining companies will face almost identical risk, it is how you manage and mitigate those risks and use them to your advantage where possible that matters (Respondent 5)
Organisational Culture	<ol style="list-style-type: none"> 1. Culture came out as one of the challenges in ERM implementation and it is tied to the maturity of the organisation. 2. ERM is changing the culture of the organisation 	<ul style="list-style-type: none"> - From an outsider's perspective, [like risk consultants and auditors], we are doing fantastic things! You know why? Because they can come in and tick those boxes [for compliance], but I always want to say from a risk culture point of view we are not doing that fantastically, because still it is difficult to get people to really be passionate about risk management. So that is where the challenge lies (Respondent 8) - When I took over it was very haphazard, the culture now is good, risk is on everyone's agendas, it's discussed, it is definitely a factor, the risk process informs many different processes, and we have still got a long way to go in terms of maturity.." (Respondent 12) - ERM is changing the culture of the organisation (Respondent 2)

5.7 Conclusion

The research questions, together with the themes that emerged from interviews are provided below in table x, summarising the results for this chapter.

Table 5: Research question, emerging themes and summary themes

Research Question	Emerg ed Themes	Summary Main Themes
1. To what extent have organisations adopted a formal enterprise-wide approach to risk management and why did they adopt it?	<ol style="list-style-type: none"> 1. Current approach to enterprise risk management 2. Mining industry has a developed statutory framework which they comply with. 3. Enterprise Risk management viewed as a business imperative 4. A need for more integrated view of risk 	<p>All research participants indicated that there is an enterprise risk management approach in place.</p> <p>Due to the nature of mining, the compliance factor plays an important part to a mine's functionality, and research participants indicated that compliance formed an important reason why they adopted ERM.</p> <p>However, the focus is now shifting to ERM being seen as a strategic business tool for those who have adopted it. It is moving them away from the practice of relying heavily on financial risk indicators to determine the successes of a business.</p>
2. How does ERM enhance an organisation's internal control system?	<ol style="list-style-type: none"> 1. Understanding enterprise risk management as a key component of the business strategy 2. ERM enhances internal control system through improved focus on the right risks 3. Internal audit is an important aspect of internal control, driven by ERM 4. Other control improvement measures 	<p>The understanding amongst most of the research participants is that ERM improves the internal control system, however, in practice; not all research participants experience it.</p> <p>Most of the research participants pointed out the importance of having an internal audit, integrated risk and control reporting, Exco-level ownership of risk and controls and cost efficiencies as other important measures of how well the organisation is managing the internal control.</p>
3. What are the key factors in ensuring that ERM enhances an organisation's internal control system?	<ol style="list-style-type: none"> 1. The role of senior manager and others in leadership positions is paramount to the advancement and successes of ERM within organisation. 2. The maturity levels of ERM within organisations goes a long way to seeing the true value of this process. 	<p>Research participants identify the role of senior managers and others in leadership positions as important to the adoption and success of ERM.</p> <p>Organisations that have adopted ERM highlight that there is a difference in maturity levels of ERM within organisations and a mature ERM process can bring true value to risk management process, particularly if it is to improve internal control.</p>

CHAPTER 6: DISCUSSION OF RESULTS

6.1 Introduction

The purpose of the discussion of the results is to determine how the ERM approach adopted by organisations has enhanced the internal control system of the organisations in the mining industry of South Africa, especially in light of the theoretical base presented in the literature review in Chapter 2.

In the literature section, the phenomena of ERM and internal control were extensively explored and this chapter aims to interpret the findings from the data collected in Chapter 5 with theory of ERM and internal control as captured in Chapter 2. This is done in order to understand if these phenomena within the South African mining industry share the same aspects or even provide additional insights. The results were concurrent with the literature on many levels, but surfaced few new findings, and contradicted the literature on some points. Each of the research questions is discussed separately below and includes explanations of where the data overlapped and departed from previous research as well as where the data provided new insights that the current literature has not covered.

The research results discussed in this chapter demonstrate that this study contributes to the existing ERM and internal control body of knowledge.

6.2 Research Question 1

This research question sought to determine the extent to which organisations have formally adopted the ERM framework and why they adopted it. The aim is to establish a sound basis for evaluating the impact that ERM has on the internal control system, covered in section 6.3.

6.2.1 Interpretation of results

6.2.1.1 Reasons for adopting ERM framework

Regulatory compliance appear to be the key driver of ERM, strategy is an emerging driver of ERM programs

It emerged from the literature that ERM still means different things to different people; to others it is just a compliance/ tick-box exercise, to others a corporate governance

requirement and others an instrument that can help an organisation to manage its risk (Arena et al., 2011). The data indicated that compliance formed an important reason why mining organisations adopted ERM. ICMM (2012) affirms that due to the nature of mining, the compliance factor plays an important part to a mine's functionality. Noncompliance with regulatory requirements could result in forfeiture of mineral rights. Furthermore, mining is a hazardous activity. Apart from personal suffering, work-related injuries could lead to a shutdown of operations resulting in lost production and jeopardise the company's licence to operate.

However, the focus is now shifting to ERM being understood as strategic business tool for those who have adopted it. ERM is seen as no longer about just ticking the boxes for compliance or for corporate governance requirement purposes; it is seen as business imperative. There is recognition that what sits at the heart of good risk management is achievement of strategic objectives and organisations are now integrating ERM into strategic planning.

A need for a more integrated view of risk, away from the functional and per discipline silo-based risk was another element that came out from the data. Traditionally, the mining organisations have placed more emphasis on safety and health risk management and with the integration of risk across all organisation's functions, levels and disciplines, a more integrated view of organisational risks has helped organisations to be better informed when making strategic decisions. This means that organisations no longer want to deal with narrow range of risks on a largely compartmentalized and decentralized basis, but rather view all risks together within a coordinated and strategic framework (Nocco & Stulz, 2006). This is reflected by the diversity of risks that are in scope of the ERM program as seen in Appendix 1.

6.2.1.2 Extent of ERM adoption in organisations

No academic literature was found regarding the current extent of ERM in mining organisations, especially in South Africa. This is indicative of the current knowledge base around this topic. The only relevant literature that was referred to was a study performed by Beasley et al. (2011) who studied different types organisations globally, covering large size organisations (those with revenues at \$1 billion or greater), public companies, and financial services entities, and Coetzee and Lubbe (2013) who compared private sector JSE listed organisations and the public sector organisations in South Africa.

The study by Beasley et al. (2011) indicated a modest trend towards more advanced enterprise-wide risk oversight from 2009 through 2011. The study found that despite the growing demand for more effective risk oversight that has emerged from the recent financial crisis, the level of enterprise-wide risk oversight across a wide range of organisations remains fairly immature. This is an interesting observation as the data from Chapter 5 indicated a much more mature ERM practices within the mining industry; ERM maturity levels are between intermediate and mature levels. This is more aligned to the study by Coetzee and Lubbe (2013) which found that that South African JSE listed private sector organisations are on average risk mature. All the mining organisations included in this study are private organisations and majority of them are listed on the JSE.

The higher ERM maturity levels of the mining organisations can be attributed to the fact that the industry has long been characterised by regulatory compliance requirements and therefore had to implement certain risk management measures to comply. This is concurrent with Sarens and Christopher's (2010) view that companies operating in a complex industry such as mining are expected to have more developed risk management and internal control systems.

While the findings demonstrate maturity in ERM, more still needs to be done. For instance, the challenges that Beasley et al. (2011) attributed to the fairly immature levels of maturity in their study are consistent with the findings of this study. These challenges include, achieving greater penetration and integration of risk management into business processes, facilitating a risk-aware culture, and developing tools and systems to support risk management. The data showed that even mining organisations are still experiencing similar challenges as seen in Table 3 of Chapter 5. Therefore, there is an argument to be made that the siloed approaches to risk management that existed previously may have resulted in the different risk management processes and practices in the respective functional areas such as finance and safety, as an example. Thus, while ERM may be bringing a uniform approach to risk it may be hampered by these legacy system issues and other change management challenges.

Furthermore, Coetzee and Lubbe (2013) acknowledge that "Although it would seem to be a fair assumption that all organisations would want to strive for the highest risk maturity level, this may not always be the case..." (p.46). For example, from the data, it is clear that there is a concerted effort being made towards ERM and there is also a recognition that there is more that needs to be done when it comes to ERM even

though South Africa has more risk management capabilities than other countries as demonstrated by the following quotes (restated from Chapter 5):

“I don’t think there are many other countries that does it as well as we do in SA. I am talking risk management more than internal audit. I am not a risk manager so I am not bragging; I am complimenting the risk management people in SA”
(Respondent 5)

“Enterprise wide risk management, I think companies are starting to get there. There are very few companies that I think are even 70% where they should be, I think we are at about 65%, and I think we are fairly mature compared to others because you find that unfortunately with risk management, very often it is a very narrowly driven process, from a corporate head office, where a couple of people sit and sort of advice the rest; then you get to a site, a business unit, and they either don’t know about it or it is stuff that gets given to them by corporate, and it doesn’t come from that side as well” (Respondent 12)

The literature provided a basis for evaluating the extent to which ERM has been adopted in organisations, through the ERM Maturity Capability characteristics identified by various authors (Beasley et al., 2011; IMA, 2011; Coetzee & Lubbe, 2013; MacGillivray et al., 2007). Consistent with the acknowledgement above that more still needs to be done when it comes to ERM, the data showed that not all characteristics of the ERM maturity capability were implemented at mature levels.

Coetzee and Lubbe (2013) and Ionescu (2008) assert that risk maturity is dependent on organisational requirements and that it may not be necessary for a specific organisation to implement all the elements of a risk management framework in order to manage its risk effectively and efficiently. However, the data showed that these different maturity levels were not as a result of organisations choosing not to implement certain characteristics, but rather contextual elements influenced the maturity of the characteristics as explained below.

In Chapter 5, the data showed that organisations are more mature in the ERM maturity characteristics that talk to the governance aspects of ERM, than the process, people and technology aspects. On the aspects that talk to process, people and technology, the data showed that organisations are still battling to integrate ERM with other business processes such as performance measurement, communication and the overall culture, to fully institutionalise ERM in the organisations. Kimbrough and Compton (2009) pointed out that the culture of an organisation can be major

impediment when implementing ERM. In addition, Jokipii (2010) argues that organisational growth increases communication and control problems, while Sarens and Christopher (2010) on the other hand suggest that larger companies are expected to need more developed risk management and internal control systems.

However, it is acknowledged that it may take longer for these companies to develop such risk and control systems as size of the company and the number of geographical locations have an influence on how quickly these can be developed. Given the large size of the mining organisations included in the study, ranging from the smallest being 4 500 employees to largest being 60 000, it can be concluded that the mining organisations are on an upward trajectory of maturing their ERM practices, given that majority of them only commenced with their ERM efforts less than five years ago.

Bottom-up versus top-down approach to risk management

Additional findings came out from the data which provided new insights that the literature did not cover. These are issues around top-down versus bottom-up approach to ERM. While the data indicated that ERM in mining has developed, organisations perform the top-down risk management very well, however they are still experiencing challenges with the bottom-up approach. This means that there is a disconnect between the operational mine-specific, process-specific risks and the corporate risks. Risks emanating from the strategy are being identified with ease and get reported on readily (top-down) while risks emanating from operational processes at the mines (bottom-up) are difficult to identify and feed them to the overall enterprise risk register.

Deloitte (2010) acknowledge in their paper that the challenge is to establish the connection of the “top-down” identified risks with the operational risks people encounter in their day-to-day activities and that once this is accomplished, risk management can be truly embedded into the organisation, making it part of daily processes and operations. This means that structures need to be designed where operational risk information can feed up to the higher enterprise-level risks required for informed “top-down” management of the organisation’s risks. Furthermore, the enterprise-level risk information that has been compiled needs to also be fed down, translating it into concrete activities on the operational work floor required for effective bottom-up management of specific exposures.

The ability to measure and manage risk exposures from both the top-down and bottom-up is critical to becoming a fully ERM mature organisation, mainly because there may be very different risk types associated with each approach; the former may

address 'big bet' risks such as geopolitical or markets issues shaping the company performance, while the latter emanates from the operational environment and may address issues such as bad debtors or employee safety and this risk approach can help the organisation to identify a weak operational procedure.

6.2.2 Conclusion to research question 1

The data from the study largely supported the literature in evaluating the extent to which organisations have adopted a formal enterprise-wide approach to risk management and why they adopted it. The data provided evidence of a formal adoption of ERM practices in mining organisations, based on the mature levels that these approaches are at. The literature outlined several reasons why organisations adopt ERM but what emerged from the data was that due to the highly regulated nature of the mining industry, compliance formed an important reason why they adopted ERM, but the focus is shifting to ERM being recognised as strategic business tool that will enable the achievement of the organisation's strategic goals.

Thus, the finding that the maturity levels are between intermediate and mature is no surprise, particularly due to the complex nature and status of mining industry that requires an integrated ERM to be formally adopted as a business imperative (Jokipii, 2010). To this effect, the higher ERM maturity result that came out from the data, provided a sound basis to better understand how then the ERM system that is in place has impacted the internal control system of those organisations and this is discussed in the next section.

6.3 Research Question 2

Research question two aimed to determine how the ERM approach implemented enhances the organisation's internal control system.

6.3.1 Interpretation of results

The literature that explores the relationship between ERM and internal control system has not been explored previously. Previous research has focused mainly on the relationship as it pertains to the maintenance of effective internal controls over financial reporting. Academic knowledgebase of both ERM and internal control is limited. Even more so, from a South African perspective, particularly in mining, it is almost non-existent. Selto and Widener (2004) analysed published research and found that there were fewer internal control topics in the internal control research literature. Jokipii

(2010) also found that the professional literature on internal control has made progress towards developing international control frameworks, but the amount of internal control research is limited.

The available literature that has been reviewed implied that ERM improves internal control, which in turn helps the organisation to achieve its strategic objectives, particularly due to the shift from the silo-based traditional risk management to ERM. For instance, there are conceptual arguments that the internal control system relies on the risk management system to identify the risks that need to be controlled. (Arena et al., 2011; Cappelletti, 2009; Gates et al., 2012; Vijayakumar & Nagaraja, 2012). Moreover, an effective system of internal control is grounded on adequate and comprehensive analysis of enterprise-wide risks (Lin & Wu, 2006; Rae et al., 2008). What was missing from the literature was that, if this is the case, how then does ERM enhance the internal control system?

The findings from the data revealed that ERM brings greater improvement to internal control, and more importantly, it is a strategic tool that can also influence how the business functions in the future.

Detailed findings on how ERM has improved internal control are discussed in the following paragraphs.

The strategic focus of ERM improves internal control

The data indicated that there has been a significant shift in the way business views risk management. The argument has moved beyond looking at the financial indicators as the only key component to business success. Organisations are now starting to question the sustainability of their current business models and what they should be controlling in order to mitigate the risks that will affect the way they do business. More importantly, they are asking how to control and manage these risk factors.

This finding is consistent with the literature which has argued that there is greater emphasis being placed by organisations on improving internal control systems (Jokipii, 2010; Rae et al., 2008). The data adds to the literature by asserting that ERM with its strategic focus has enabled the enterprise-wide view of business risks, together with the enterprise-wide design and management of internal controls, although not in an integrated manner as it should. If organisations do not have proper controls, they are very unlikely to achieve their strategic objectives. The data emphasised that this is the

one area of risk management that many people do not fully grasp, that the risks must be defined in the context of the business objectives.

What is key is being able to determine comprehensively all the risks that are going to prevent the business from achieving those objectives, and that is the role of ERM. This then allows the organisation to put in place all the control measures that will help control the risks. Controls now have more meaning as to which risks they are controlling and for which business objective they are helping achieve. The data supports the literature that the various corporate governance guidelines that exist have also placed significant emphasis on an organisation's approach to risk management as a key mechanism that overarches the design of internal controls throughout the organisation (Rae et al., 2008).

ERM enhances internal control system through improved focus on the right risks

Internal controls improvement relates to how rigorous the controls for given processes or activities are in managing the risks associated with those processes or activities, and whether they are sufficiently documented and efficiently maintained, assessed, and reported (Dietz & Snyder, 2011). From the data, there is a strong emphasis placed on identifying the risks that can be controlled. ERM creates the focus by management on the right risks and on the right controls and their effectiveness. If controls for example are found to be ineffective, there are actions that are taken and this results in the overall control environment improving.

Furthermore, the data revealed that prior to implementing ERM internal controls were "badly" designed. Since internal control system design is management's responsibility (PricewaterhouseCoopers, 2007; Rae et al., 2008), management need to know at what levels the internal controls need to be, so the benefit of ERM is that it provides management with this knowledge to be able to design appropriate internal controls to control the correct risks. Therefore, the conceptual arguments presented by Lin and Wu (2006) and Rae et al. (2008) that an effective system of internal control is grounded on adequate and comprehensive analysis of enterprise-wide risks have been validated by this data.

The findings further demonstrated that there are linkages between the various risk exposures of the mining organisations and these range from the sustainability issues that talk to communities, environmental, safety, and health which overlap with other functions and disciplines such as human resources, security, and finance; ERM has

thus been able to break down the silos which existed between them and has helped improve the overall control environment through the process.

Understanding of Internal audit as an important aspect of internal control

The data indicated that internal audit is an important component of internal control in the business and that through ERM, the value provided by internal audit has improved and ties to the risks pertinent to the achievement of the organisation's strategic objectives. The finding supports the literature in that since the advent of ERM, internal auditors have been encouraged to take on a new and potentially more valuable role in their organisation's approach to ERM (Rae et al., 2008). The literature further expands that the changing role includes following a risk-based approach to internal audit as it allows internal audit to determine whether controls are effective in managing the risks which arise from the strategic direction that the organisation has decided to take and providing assurance on the risk management processes. The findings further reveal that organisations are beginning to perform more non-financial assurance than financial. The focus has shifted from only auditing the financial controls.

Furthermore, the assurance process has moved away from just mapping out the organisational processes and auditing controls in those processes, it is now determined by the key risks of the organisation. This means that there is more understanding of how the assurance process impacts the organisation's objectives.

Improvements through the integrated risk and control reporting

Deloitte (2010) in their Enterprise Risk Management Benchmark Survey conducted across the Energy & Resources Industry in Europe, Middle-East and some parts of Africa, found that many organisations still struggle with monitoring and reporting risks. A lack of appropriate tooling was one of the reasons. Other reasons were the lack of suitable methodology for aggregating risks, the lack of ability to measure and integrate reporting of risk exposures from both the top-down (organisational level) and the bottom-up (operational level). This is an interesting observation in that the data stressed the importance of having an integrated risk and control reporting, as an important measure of how well the organisation is managing the internal control, thus managing the risks that threaten achievement of objectives. The reporting that is currently being done integrates risk, strategic objectives and internal control and shows if there is a decline in the number control failures as was the case with some organisations. The reporting is however geared more towards the top-down risks and

supports the Deloitte (2010) finding of a lack of ability to measure and integrate reporting of risk exposures from both the top-down and the bottom-up.

Risk and Control ownership at Exco level

Risk and control ownership at Exco level emerged from the findings as one of the benefits brought about by ERM. Blaskovich and Taylor (2011) concur that the board delegates the responsibility for owning and managing risk with the Chief Executive Officer (CEO), and, by delegated authority, with executive and line management of the organisation. However, the data showed that the level of accountability varies and in some instances promotes over-reaction as summarised below.

- There are risk owners and control owners per risk at Exco level tied to their KPI's.
- The extent to which there is proper accountability and consequence management seems to be low, raising concerns of whether the ownership is really there.
- There is very fine line between management taking the responsibility to sort things out, and over-reacting. The over-reaction is evident when management is hiring their own audit teams to go and audit themselves, to make sure that when internal audit comes to audit, they don't receive inefficient or weak reports on their control environments.

Improved cost efficiencies

In the literature, Ionescu (2008) outlined some of the challenges that organisations are faced with when it comes to prioritising and ensuring that there are no duplications in internal controls which may result in cost inefficiencies. Significant effort and costs are expended by organisations to build controls that address potential risk. However, in most cases the correlation, intersection and duplication of controls across different groups are not clearly visibly or easily understood because of the siloed approach that many organisations have taken in the past towards risk management. It is interesting that the literature highlights these challenges whereas the data does not support this. The majority of the responses from the data did not highlight this as a challenge. Only two respondents had experienced the improvement in cost efficiencies because any capital budget requirements must be to significantly control a major risk exposure. In addition, through the improved assurance process, the number of the various external assurance services that the organisation was utilising to review the internal controls for compliance has decreased, resulting in a rand value saving for the organisation.

The fact that the data did not support the literature in this regard could be attributed to reasons that perhaps the maturity of the ERM practice has not reached this stage yet of evaluating ERM cost versus ERM return and the interview process did not probe further on this issue.

Relationship between improved internal control with achievement of strategic objectives

An interesting observation to note is that although not explicitly investigated, the literature inferred the relationship between an improved internal control system with achievement of strategic objectives (Vijayakumar & Nagaraja, 2012). However, the findings provided additional insights in that there is no clear evidence of how strategic objectives are being achieved as a result of the improved internal control. To realise this improvement, more time is needed to be able to measure this aspect. The researcher concurs with the findings as majority of the mining organisations in the sample only commenced with their ERM efforts less than five years ago. This also talks to Jokipii's (2010) finding that evidence of the actual performance of an internal control system within the organisational environment is almost non-existent and that the topic is relatively unexplored by researchers. This can be considered to be an area for further research in this field.

6.3.2 Conclusion to research question 2

The literature that explores the relationship between ERM and internal control system is non-existent, thus this research question based its findings on the conceptual arguments that the internal control system relies on the risk management system to identify the risks that need to be controlled. Moreover, an effective system of internal control is grounded on adequate and comprehensive analysis of enterprise-wide risks. These conceptions were validated by the data with additional findings that expanded on the literature by demonstrating that ERM brings greater improvement to internal control. Thus, the findings provided a better understanding of how the implemented ERM improves the internal control system of organisations.

6.4 Research Question 3

This question follows on research question two in that it sought to better understand, more especially from those organisations that have more mature ERM practices in place, what the factors are that ensure that ERM enhances an organisation's internal

control system. More importantly, to find out what the key factors might be that could affect the success of ERM and its benefits to the control system of the organisation.

6.4.1 Interpretation of results

Research questions two above demonstrated that indeed the implemented ERM does enhance the organisation's internal control and provided evidence of those improvements. While this research has taken into consideration the contingency arguments presented by Ionescu (2008) and Jokipii (2010), that every organisation has different internal control requirements, circumstances and objectives, and that the ERM application also varies depending on the organisational contexts, certain factors emerged from the data that organisations should take into consideration and plan for them in order to ensure that the implementation of ERM realises the intended benefits, including those of enhancing the internal control system.

The literature has not emphasised specifically on the key factors critical in ensuring that the deployed ERM approach enhances the internal control of organisations. Therefore, the findings presented below add to the literature by providing an enhanced understanding of what is critical in ensuring that ERM enhances an organisation's internal control system.

The role of leadership is paramount to the advancement and successes of ERM

The data stressed that implementing a new system as immense as ERM that changes how an organisation conducts its business, more so if it is intended to help an organisation be more resilient in times of uncertainty, it requires buy-in from top-management. There is a need to obtain organisational buy-in, and this goes all the way to top-management. What was abundantly clear from the data was that the type and quality of the leaders play a huge role in how ERM efforts are to succeed. EXCO need to believe in the process.

An interesting observation to note from the data was that the tone at the top is important; it is a necessary condition, however the tone alone is not going to achieve results; the ability to drive ERM into the organisation and to change the consciousness of each individual employee or stakeholder is more critical. Thus, what the leaders communicate and how they communicate is critical, they must have the ability to translate the ERM messages from the top such that they effectively permeate into the organisation and everybody else can live that culture. This is where the quality of the CRO becomes critical as well. These findings support Coetzee and Lubbe (2013) that

with regard to the organisational culture, leadership from senior management and the governing body to incorporate a risk mindset into the organisation's culture are a critical element in the drive to achieving an effective risk management framework.

The below paragraph from the literature provides a view of the roles performed by the leaders in the organisation with regard to risk and control.

While the organisation's board of directors are ultimately accountable for risk and control within the organisation, It can be drawn from the literature that explained the various roles and responsibilities for risk and internal control are three pronged functions as follows: (1) the taking of risk is undertaken by the organisation's board, and the management of system of internal control is driven by the CEO, with delegated authority to his Exco and line management; (2) the observation and support of risk management, is undertaken by the office of the CRO; and (3) the monitoring and audit of risk management and associated internal control, is undertaken by the office of Internal Audit (Acharyya, 2006; Blaskovich & Taylor, 2011; Rae et al. 2008). The data supports the literature as these roles and functions are being followed in the sampled organisations.

The maturity levels of ERM goes a long way to seeing the true value of the process

The data indicated that the true value of ERM is diminished when the level of ERM maturity within organisation is minimal. As pointed in the above section, that there are other key factors such as senior managers and leadership buy-in that is required in order to have the desired impact of ERM on the internal control system, more importantly, the quality and the maturity of the ERM process is what kills or propels the entire process. The literature points out that while ERM practices from a South African private sector perspective are more mature (Coetzee and Lubbe, 2013), ERM practices globally are less developed (Beasley et al., 2011), and more evidence is needed to understand the constraints that exist that prevent organisation from operationalizing ERM to an extent that improvements on the internal control are realised.

Other factors within the context of ERM maturity were explicit from the data and these are discussed below.

The risk culture plays a huge part in how successful organisations are in driving ERM and internal control focus. Organisations need to be able to adapt quickly and a means to be able to do so if people think proactively all the time as changing the risk culture is

what takes time. Therefore, there is a need to change the organisation culture if ERM is to become the heart of the organisation. The data supports the literature as concluded by Kimbrough and Compton (2009) that, organisational culture is one of the top barriers to the success of ERM programs. It appears from the data that a combination of organic and mechanistic qualities exists in the culture of the organisations. The organic culture fosters collaboration, lateral communication, and employee commitment to the organisation's tasks while the mechanistic advocates adherence to standards mandated from the top, compliance with rigorous activities of regular risk assessments and control activities, employees needing detailed instructions, and a hierarchical chain of command.

The mining industry may have been successful to an extent with the mechanistic culture in the past due to its compliance-based approach, however, as Kimbrough and Compton (2009) explain, the shift from the tradition of managing risk within organisational silos to managing risks on a portfolio basis across the entire entity leads to a requirement for effective communication and collaboration across the organisation. ERM assumes that identification and communication of risks will occur freely and that there will be "risk transparency throughout an organisation". Therefore, a more organic culture needs to be nurtured. This recommendation is supported by Brodeur and Pergler (2010) who encourages a culture where risk is considered a core part of managers' responsibilities and where ERM is anchored by strong individual risk-related managerial processes for example where appropriate risk analyses are embedded into normal management practices, to a point where the risk culture permeates the enterprise.

An interesting recommendation from the data is that of a simple ERM process. It is suggested that organisations need to keep the ERM process as well as the ERM tools simple as most of the enterprise risk management skills in mining are low and employees at the lowest level must be able to understand what is risk management. This is interesting to note, particularly as the various frameworks alluded to in the literature have outlined the ERM process (See Appendix 4) for the two ERM guidelines that are generally followed, COSO 2004 and ISO31000). An implication from the data is that the industry finds these processes to be complex. The question then is 'Will the industry be better off with a simple process or false hope is being provided that ERM is simple?'

The factors outlined above can be used to explain the challenges that Beasley et al. (2011) found in his ERM maturity study of global organisations, particularly because

issues of leadership and maturity of the ERM process are central to achievement of an initiative like ERM. As alluded to by Beasley et al. (2011), issues of organisations not being able to achieve greater penetration and integration of risk management into business processes, measuring and aggregating risk and development of tools and systems to support risk management together with being able to facilitate a risk-aware culture (Kimbrough & Compton, 2009), all speak to the question of having the right leadership and a mature ERM process.

6.4.2 Conclusion to research question 3

With this research question, the research paper aimed to obtain additional insights that were specifically on those factors that affect the success of ERM in enhancing the internal control system of the organisation. The role of leadership and the maturity of the ERM process are paramount in institutionalising ERM. Within the maturity of ERM process, aspects of culture and a “simple” process go a long way in ensuring the success of ERM and its benefit on the internal control. Factors of leadership, maturity of ERM and organisational culture, on their own have been researched in organisational and risk management research but were not pre-empted or hypothesised as the very nature the research was to obtain additional insights from practice that can contribute to the existing literature.

6.5 Conclusion

The objective of research was to determine how ERM affects the internal control system of the organisation and this objective was met by answering all the three research questions. The existing limited literature was supported by the findings and overlaps were highlighted together with additional insights that were not explicitly covered by the literature. The very nature of the research allowed new insights to be explored and brought to the fore. From synthesising the data on all aspects of how ERM and internal controls are being managed in the sampled organisations, together with the available literature and what the ERM frameworks are advocating, conclusions can be made that description of ERM and the implementation process can portray ERM to be an onerous process for managers than it actually is. Following on the views by Galloway and Funston (2000), ERM can be a simple process if every business unit manager is able to say:

“Here are the top ten risk issues for our team and this is how we are acting on them. The process takes about two to three hours our management team’s time to perform formal assessments every quarter.

Here are our top strategic initiatives to market opportunities and challenges, and these are accompanied by an assessment of risks to these initiatives, and how we are acting on them.

Everyone in my team knows their role in controlling the risks through the key controls process that is informed by this risk assessment – and here is how we are doing it (Assurance can validate).

All our risk and control information is held on our ERM database, which gives us up-to-date risk profiles and scorecards for our units and is accessible when we need it”

If every business unit manager in the organisation can outline this as part of how they run their business, this can eliminate a lot of fire-fighting of unexpected problems and can provide more (but not absolute) certainty that the achievement of organisation’s strategic objectives will be met. This sounds simplistic, but the data suggests that it is that simple, particularly given that ERM practices in the mining sector are already at intermediate to mature levels. Therefore the level of effort required will not be as intense as it would be if they were at immature stages of ERM.

CHAPTER 7: CONCLUSION

7.1 Introduction

This chapter briefly reviews the research problem and objectives set at the outset of the project, before summarising the main findings and then presenting a model for enterprise risk and control convergence. This model is presented as a result of the findings and insights garnered from the respondents, as discussed in Chapter 5 and Chapter 6. Recommendations to the various stakeholders are then provided together with implications and recommendations for future research, followed by conclusion to the research report.

7.2 Review of research objectives

The relevance of this research was established in Chapter 1 and Chapter 2, with recent studies alluding to the need for ERM and an improved internal control system. In a mining industry context, the application of risk management has been advocated by compliance requirements, however, the shifting social, economic and political trends have changed the operating efficiency of mining organisations with the scope, complexity, and interdependencies of emerging risks necessitating a more robust and integrated approach to risk management and internal control.

The purpose of this research has therefore been to understand how the ERM approach adopted by organisations in the mining industry has impacted their internal control system, which in turn is implied to help organisations to meet their strategic objectives, thus improving performance. In order to reach the objectives, the research explored the extent to which organisations have adopted a formal enterprise-wide approach to risk management (ERM), established why they adopted it, determined how this ERM adoption impacts the internal control of the organisations and identified key factors that are critical in ensuring a positive impact of ERM on an organisation's internal control system. The results of this research provided additional insights that will bolster a successful advancement of internal control management through ERM.

7.3 Major findings

Within the mining industry, regulatory compliance appears to be the key driver of ERM and strategy is an emerging driver of ERM programs. The findings reflect that

compliance formed an important reason why mining organisations adopted ERM. Due to the nature of mining, the compliance factor plays an important part to a mine's functionality. Noncompliance with regulatory requirements have implications on the organisation's continued existence. The scope, complexity, and interdependencies of emerging risks alluded to above in section 7.2 have shifted the focus of ERM to being understood as strategic business tool for those who have adopted it. It is no longer about compliance or for corporate governance requirement purposes; it is seen as business imperative.

ERM frameworks are becoming more mature and are achieving enterprise wide coverage. There was overall consensus in the findings that organisations have an ERM practice that has progressed beyond its early stages. The fundamentals of the ERM program such as the framework and tools have been established and serve as the basis for the development of more advanced risk management practices. It is to be noted that although much progress has been made in maturing the ERM practices particularly the governance aspects of ERM, organisations have not fully integrated ERM with other business processes such as performance measurement, communication and the overall culture of the organisation. Thus, while ERM is bringing a uniform approach to risk, it could be hampered by legacy issues of silo-based risk management and other challenges involving change management.

Further insights on the aspects of top-down versus bottom-up approaches to ERM were highlighted by the findings, reflecting the challenge that mining organisations are having with bottom-up approach. This indicates a disconnect between the operational mine-specific, process-specific risks and the corporate risks. Integration of risk into all business processes is fundamental for ERM success and its institutionalisation.

Overall, ERM brings improvement to internal control systems of organisations; particularly its strategic focus has enabled the organisations to focus on the right risks. The focus has moved beyond looking at the financial indicators as the only key component to business success. Organisations are now starting to question the sustainability of their current business models and what they should be controlling in order to mitigate the risks that will affect the way they do business.

ERM has enabled the enterprise-wide view of business risks, together with the enterprise-wide design of internal controls, although not in an integrated manner as it should. The view is that if organisations do not have proper controls based on the right

risks, they are very unlikely to achieve their strategic objectives. However, additional insights were noted that there is no clear evidence of how strategic objectives are being achieved as a result of the improved internal control and this was attributed to lack of enough coverage period to be able to measure this aspect.

There is a strong emphasis placed on the role of internal audit as an important component of internal control in the business. Through ERM, the value provided by internal audit has improved and ties to the risks pertinent to the achievement of the organisation's strategic objectives. The focus has shifted from only auditing the financial controls; organisations are beginning to perform more non-financial assurance. The reporting capability of organisations has improved with ERM, as the reporting now integrates the enterprise risks, their impact on strategic objectives and the status of the internal controls put in place to manage those risks that will affect the strategic objectives.

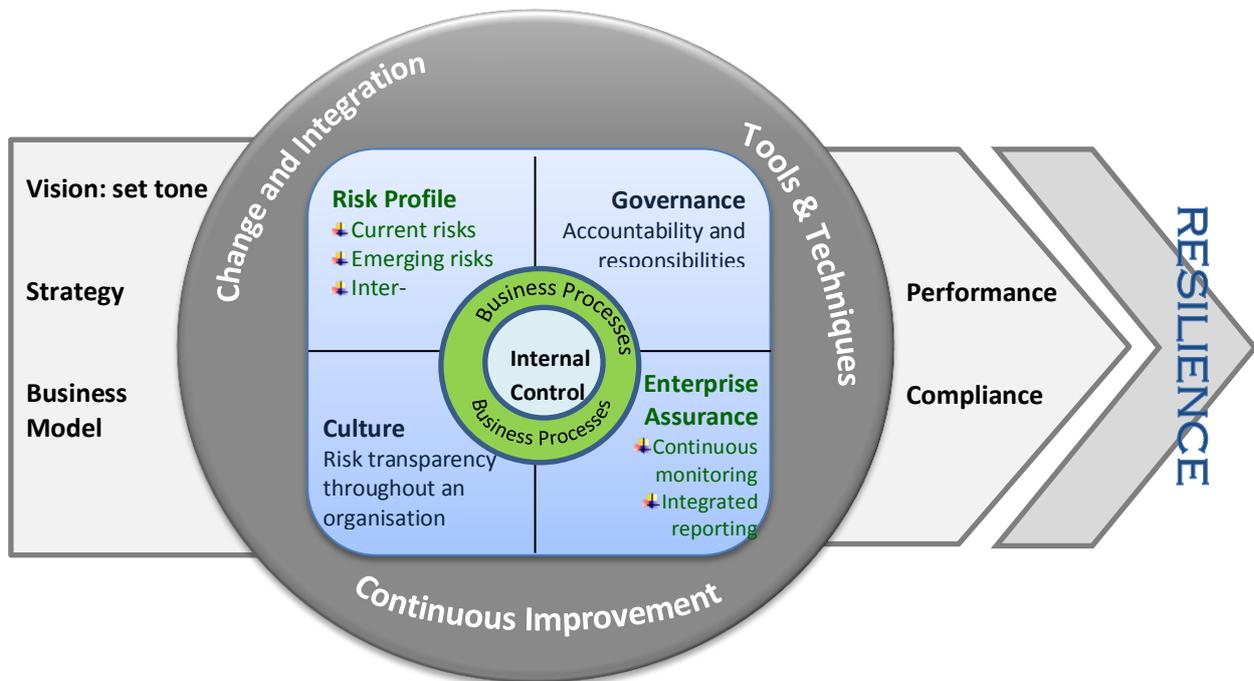
Risk and control ownership at Exco level emerged as one of the benefits brought about by ERM, however, the level of accountability varies, in some instances the level of accountability is questioned and on the other hand management over-reacts by getting various teams of auditors to audit their control environments prior to official scheduled audits that get reported at Exco. The type and role of leadership and the maturity of the ERM process are identified as the key factors that affect the success of ERM and its benefits to the control system of the organisation. Particularly for the mining sector, the right risk management messages from the top delivered in a manner that can be comprehended by the lowest level employee and through a simple process can go a long way in institutionalising enterpriser risk management.

7.4 Enhancing and sustaining the ERM capability

Enhancing and sustaining the ERM capability at most organisations in the mining industry will require a process of continuous improvement. Changes in prevailing conditions in the mining industry's operating environment, the organisation's objectives and the expectations of key stakeholders may require additional effort to enhance and maintain the desired ERM capability maturity. To this effect, Figure 6 shows a model for enterprise risk and control integration and was constructed by synthesising the findings of this research. The model illustrates the key elements that make up an integrated enterprise risk and control framework. This framework can be used by management, risk management practitioners, internal auditors and academics to

increase the probability of ERM success and its intended benefits on the internal control system.

Figure 6: A Model for Enterprise Risk and Control Integration



The left hand side of the model shows that an organisation sets a vision that serves as the tone for the entire organisation to ensure risk information is incorporated into the critical decision making about the strategy of the organisation and how it will conduct its business. Inside the circle shows the integrated risk and control environment with strategy at tactical and operational levels where internal controls as the heart of the business, are incorporated into the key business processes that help the organisation to achieve its strategic objectives and all key processes are linked to the risks. This is done through establishing the risk profile of the organisation, the right culture, proper governance models for risk and controls and the integrated assurance from internal audit and external assurance parties, providing the continuous monitoring and integrated reporting. These are supported by change and integration initiatives, ERM tools and techniques such as methodologies and technology and continuous improvement. The right hand side of the model shows the resulting effects of ERM performance and improved compliance. The framework can help an organisation to be more resilient in times of uncertainty.

It is to be cautioned however that this model is not a panacea for managing enterprise risk, but a guide for ensuring that each of the elements critical in the program are addressed, mainly because every organisation has different internal control

requirements and objectives, and the ERM application also varies depending on the organisational contexts.

7.5 Recommendations for stakeholders

The recommendations made are based on what has been observed as currently working well within the industry, as well as new recommendations that have been identified through the findings.

7.5.1 Recommendations for management and boards of directors

This research provides additional insights for management and the boards of organisations to strive for the on-going improvement of their risk preparedness and effective corporate governance to achieve their objective of managing and minimising risk in all their operations, to ultimately fulfil their stakeholder commitments. While the maturity levels of the ERM practices in the mining industry are at intermediate to mature levels, more work still needs to be done around improving this maturity. The fact that organisations have not fully integrated ERM with other business processes and the overall culture of the organisation is a cause for concern, particularly if organisations want to institutionalise ERM. Therefore, it is recommended that more emphasis be placed on integrating the rest of the processes around communication and performance measurement as well as building a more organic culture that will allow a risk culture to permeate the organisation.

The quality and the role of the leadership team in driving ERM efforts is paramount. An enterprise operating in the mining industry sector is constantly influenced by external and internal environmental factors, and changes of these factors may increase the risks to its performance. Trying to decrease the risks to a reasonable minimal level, there appears also a demand to establish some changes in the internal control system. The demand to improve the internal control system is fulfilled upon obtaining the right risk information from the right risk process as internal controls rely on a sound and comprehensive risk management process. Therefore, more focus needs to be placed on how the tone at the top filters through the organisation to get everyone within the organisation to understand risk management and their role in controlling the risks.

7.5.2 Recommendations for risk and internal audit practitioners

Risk management practitioners or CRO's are in charge of risk management in their organisations and have the responsibility for deploying and implementing the overall risk management program agreed upon by the organisation's board and senior

management. For this purpose, it is recommended that they establish a structured system that is both permanent and adaptable for the purpose of identifying, analysing and managing all the key risks facing the organisation and providing support to management in driving the enhancement and maintenance of ERM in their organisations. A starting point can be to apply the framework proposed in section 7.4.

Internal audit is an important component of internal control in the business and through ERM, the value provided by internal audit has improved and ties to the risks pertinent to the achievement of the organisation's strategic objectives. More non-financial assurance is being done, however, it is recommended that internal audit functions focus more on developing their audit skills to be able to provide specific assurance and recommendations on the more advanced enterprise risks in order to move risk management ahead in their organisations and ensure a sustained system of internal controls.

7.6 Recommendations for future research

The knowledgebase around Enterprise risk and internal controls is still developing in academic terms and as such, the choice of research design has been exploratory in nature. The research has therefore focused on building theory, rather than on testing that theory. Future avenues for research might include an explanatory research utilising either qualitative or quantitative methods. The research project has been aimed at uncovering insights regarding the current adoption of ERM and its impact on the organisation-wide internal control. Future research may be useful to confirm and validate the findings of this research.

The following areas of research are recommended below:

- Measuring the state of ERM adoption in mining industries of other developing and developed countries.
- Determining how internal audit functions have geared up to be able to provide specific assurance and recommendations on more advanced enterprise risks, particularly in the technical aspects of business operations.
- Investigating how the bottom-up approach to enterprise risk management can be integrated with the top-down approach.
- Further research that could be performed on ERM and internal control improvement include considering the following aspects:

- The relationship between improved enterprise-wide internal control and performance of the organisation, determining the evidence of how strategic objectives are being achieved as a result of the improved internal control.
- The correlation between ERM maturity level and the intended value it provides.
- Investigating whether the sophistication of the ERM process is dependent on the maturity of the organisation.
- Evaluating ERM cost versus ERM return on investment.
- Exploring the moral dilemma of setting risk tolerance levels in high reliability organisations, i.e. organisations that have no choice but to function reliably. If reliability is compromised, it cost the company loss of human lives.

7.7 Concluding remarks

Holistically, this research was able to explore whether ERM improves the internal control system of the organisation and how it improved it. The maturity levels of organisations in the mining industry were able to provide the basis for exploring the effect of ERM on internal control. This being the case, this research was therefore able to develop theoretical proposals for the various stakeholders of ERM in organisations as well as provide areas of future research to confirm or validate the findings.

As pointed out in the introduction of this paper, risk management has been a widely debated topic from the early days of finance research where it was considered irrelevant under perfect market conditions. However, the changing economic and business landscape results in uncertainties in today's economy. Therefore, every organisation is, to some extent, in the business of risk management, irrespective of what products or services the organisation delivers. What will give each individual organisation the competitive edge is explained by Galloway and Funston (2000) that

“An organisation that manages risk on an enterprise-wide basis will be positioned as an organisation which has risk management as a core competency, and which is able to anticipate risks better than its competitors, giving it the competitive advantage” (p.25).

REFERENCE LIST

- Acharyya, M., & Johnson, J. (2006). Investigating the development of enterprise risk management in the insurance industry: an empirical study of four major European insurers. *The Geneva Papers on Risk and Insurance, Special Issue July*, 55–80.
- Alviniussen, A., & Jankensgård, H. (2009). Enterprise Risk Budgeting: Bringing Risk Management into the Financial Planning Process. *Journal of Applied Finance*, 1&2, 178-192.
- Arena, M., Arnaboldi, M., & Azzone, G. (2011). Is enterprise risk management real? *Journal of Risk Research*, 14(7), 779–797.
- Baker, N. (2013). Fear Factor. *Internal Auditor*, 7(1) 46-51.
- Barton, T. L., Shenkir, W. G., & Walker, P. L. (2010). ERM after the financial crisis. *Financial Executive*, 26(3), 18-22.
- Beasley, M., Branson, B., & Hancock, B. (2011). Report on the current state of enterprise risk oversight. *Raleigh, NC: ERM Initiative at North Carolina State University*. Retrieved July 20, 2013 from https://www.aicpa.org/interestareas/businessindustryandgovernment/resources/erm/downloadabledocuments/current_state_erm_3rdedition.pdf
- Bernstein, P.L. (1998). *Against the Gods: The Remarkable Story of Risk* (2nd ed.). Canada: Wiley.
- Blaskovich, J., & Taylor, E. Z. (2011). By The Numbers: Individual Bias and Enterprise Risk Management. *Journal of Behavioral & Applied Management*, 13(1), 5-23.
- Blumberg, B., Cooper, D. R., & Schindler, P.S. (2008). *Business Research methods* (2nd European ed.). New York: McGraw-Hill
- Boegman, H. (2013). SA's Ming Industry. *Accountancy SA*, 34-35. Retrieved September 13, 2013, from <http://search.proquest.com/docview/1287937353?accountid=14717>

- Brodeur, A., & Pergler, M. (2010) *Top-down ERM: a pragmatic approach to managing risk from the C-suite* (Working Paper 22). McKinsey. Retrieved October 31, 2013, from http://www.mckinsey.com/insights/risk_management
- Cappelletti, L. (2009). Performing an Internal Control Function to Sustain SOX 404 and Improve Risk Management: Evidence from Europe. *Management Accounting Quarterly*, 10(4).
- Cohen, L., Manion, L., & Morrison, K. (2000). *Research Methods in Education* (5th ed.). London: Routledge Falmer
- Coetzee, G. P., & 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 Organisations (COSO). (2004). *Enterprise Risk Management- Integrated Framework Executive Summary*. Retrieved from http://www.coso.org/Publications/ERM/COSO_ERM_ExecutiveSummary.pdf
- Creamer, M. (2012, July, 04). Global mining drives 45%-plus of world GDP – Cutifani. *Mining Weekly*. Retrieved August 24, 2013, from <http://www.miningweekly.com>
- Deloitte. (2010). *Risk Intelligence in the Energy & Resources Industry: Enterprise Risk Management Benchmark Survey*. Retrieved September 15, 2013, from http://www.deloitte.com/assets/Dcom-Lebanon/Local%20Assets/Documents/Energy_and_resources/aers-erm-clientsurvey-april2010.pdf
- Deloitte. (2012). *Tracking the trends 2012: The top 10 trends mining companies may face in the coming year*. Retrieved August 26, 2013, from <http://www.deloitte.com/assets/Dcom-SouthAfrica/Local%20Assets/Documents/Industries/Mining/Tracking%20the%20trends%202012.pdf>
- Dickinson, G. (2001). Enterprise Risk Management: Its origins and conceptual foundation. *Geneva Papers on Risk & Insurance*, 26(3): 360-366.
- Dietz, D & Snyder, H. (2011). Assessing internal controls: do management and staff agree?. *Management Accounting Quarterly*, 12(2), 35-40.

- DiMaggio, P. J., & Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organisational fields. *American Sociological Review*, 48(2), 147-160.
- Donovan, D. R. (2013, May 16). Prospecting for solutions: The challenges of South Africa's mining industry. *Consultancy Africa Intelligence*. Retrieved September 15, 2013, from <http://www.consultancyafrica.com>
- Doyle, J., Ge, W. & McVay, S. (2007), Determinants of weaknesses in internal control over financial reporting. *Journal of Accounting and Economics*, 44, 193-223.
- Galloway, D., & Funston, R. (2000). The challenges of enterprise risk management. *Balance Sheet*, 8(6), 22–25.
- Gates, S., Nicholas, J., & Walker, P. (2012). Enterprise Risk Management: A process for enhanced management and improved performance. *Management Accounting Quarterly*, 13(3), 28-38.
- Giriunas, L. (2012). Evaluation of internal control system in mining industry enterprises in Lithuania. *Business Management Dynamics*, 1(12), 41-47.
- Gordon, L. A., Loeb, M. P., & Tseng, C. (2009). Enterprise risk management and firm performance: A contingency perspective. *Journal of Accounting and Public Policy*, 28, 301–327.
- Guest, G., Bunce, A., & Johnson, L. (2006). How many interviews are enough? An experiment with data saturation and variability. *Field Methods*, 18(1), 59-82.
- Guion, L. A. (2006). *Conducting an In-Depth Interview*. Retrieved from <http://edis.ifas.ufl.edu/FY393>
- Gupta, P.P. (2008). Management's evaluation of internal controls under Section 404(a) using the COSO 1992 control framework: Evidence from practice. *International Journal of Disclosure and Governance*, 5(1), 48–68.
- Gupta, P. P., Dirsmith, M. W., & Fogarty, T. J. (1994). Coordination and control in a government agency: Contingency and institutional theory perspectives on GAO audits. *Administrative Science Quarterly*, 39(2), 264-284.

- Hermanus, M.A. (2007). Occupational health and safety in mining—status, new developments, and concerns. *The Journal Of The Southern African Institute of Mining and Metallurgy*, 107, 531-538
- Heuberger, R. (2005). Risk analysis in the mining industry. *Journal Of The South African Institute Of Mining And Metallurgy*, 105(2), 75-80.
- Hoque, Z., & James, W. (2000). Linking Balanced Scorecard measures to size and market factors: Impact on organisational performance. *Journal of Management Accounting Research*, 12, 1–17.
- Hoyt, R.E., & Liebenberg, A.P. (2011). The value of enterprise risk management. *The Journal of Risk and Insurance*, 78(4), 795-822.
doi:10.1111/j.1539-6975.2011.01413.x
- International Council on Mining and Metals. (2012). *Mining's contribution to sustainable development*. Retrieved August 24, 2013, from <http://www.icmm.com/document/4441>
- International Standards Organisation. (2009). *Risk management – Principles and guidelines ISO 3100*. Geneva: International Standards Organisation.
- Institute of Directors. (2009). *King code of governance for South Africa*. Retrieved June 12, 2013 from <http://iodsa.co.za>
- Ionescu, L. (2008). Toward establishing efficient internal controls. *Economics, Management, and Financial Markets*, 3 (1), 80–84.
- Jokipii, A. (2010). Determinants and consequences of internal control in firms: a contingency theory based analysis. *Journal of Management and Governance*, 14, 115–144. doi: 10.1007/s10997-009-9085-x
- Kimbrough, R.L., & Compton, P.J. (2009) The Relationship Between Organisational Culture and Enterprise Risk Management. *Engineering Management Journal*, 21(2), 18-26.
- KPMG. (1999). *Internal Control: A Practical Guide*. Retrieved June 7, 2013, from http://www.ecgi.org/codes/documents/kpmg_internal_control_practical_guide.pdf
- Leedy, P. D., & Ormrod, J. E. (2001). *Practical research: planning and design* (7th ed.) Upper Saddle River: Merrill Prentice Hall.

- Lin, H. H., & Wu, F.H. (2006). Limitations of Section 404 of the Sarbanes-Oxley Act. *The CPA Journal*, 76(3), 48-53.
- MacGillivray, B. H., Sharp, J. V., Strutt, J. E., Hamilton, P. D., & Pollard, S. J. T. (2007). Benchmarking Risk Management Within the International Water Utility Sector. Part I: Design of a Capability Maturity Methodology. *Journal of Risk Research* 10(1), 85-104.
- Martin, D., & Power, M. (2007). The end of enterprise risk management. *AEI-Brookings Joint Center for Regulatory Studies*. August. Retrieved July 28, 2013 from http://regulation2point0.org/wp-content/uploads/downloads/2010/04/RP07-22_topost.pdf
- McShane, M. K., Nair, A., & Rustambekov, E. (2011). Does Enterprise Risk Management increase firm value? *Journal of Accounting, Auditing & Finance*, 26(4), 641–658. doi: 10.1177/0148558X11409160
- Mikes, A., & Kaplan, R. S. (2013). *Managing Risks: Towards a Contingency Theory of Enterprise Risk Management* (Working Paper 13-063). Harvard Business School. Retrieved on October 29, 2013, from http://www.hbs.edu/faculty/Publication%20Files/13-063_3803c032-e96f-40c4-8761-ea9188f502c8.pdf
- Myers, M. D. (2013). *Qualitative research in business and management* (2nd ed.). Sage Publications.
- Nocco, B. W., and R. M. Stulz. (2006). Enterprise Risk Management: Theory and Practice. *Journal of Applied Corporate Finance*, 18(4), 8-20.
- O'Connor, H., & Gibson, N. (2003). A step-by-step guide to qualitative data analysis. *Pimatisiwin: A Journal of Indigenous and Aboriginal Community Health*, 1(1), 63–90.
- Podsakoff, P. M., MacKenzie, S.B., Lee, J., & Podsakoff, N.P. (2003). Common Method Biases in Behavioral Research: A Critical Review of the Literature and Recommended Remedies. *Journal of Applied Psychology*, 88(5), 879–903. doi: 10.1037/0021-9010.88.5.879

- Power, M. (2009). The risk management of nothing. *Accounting, Organisations, and Society*, 34(6/7), 849-855.
- PricewaterhouseCoopers. (2013) *Managing Risk*. Retrieved October 12, 2013, from <http://www.pwc.com/gx/en/mining/risk-management/index.jhtml>
- PricewaterhouseCoopers. (2012). *State of the internal audit profession study*. Retrieved July 21, 2013, from <http://www.pwc.com/ca/en/risk/internal-audit/publications/pwc-state-of-internal-audit-profession-study-2012-04-en.pdf>
- PricewaterhouseCoopers. (2007). *The Internal Control System: A Rapidly Changing Management Instrument*. Retrieved June 19, 2013, from http://www.pwc.ch/en/dyn_output.html?content.void=7232&collectionpageid=3042&containervoid=25416&comefromcontainer=true
- Qu, S., & Dumay, J. (2011). The qualitative research interview. *Qualitative Research in Accounting & Management*, 8(3), 238-264. doi: 10.1108/11766091111162070
- Rae, K., Subramaniam, N., & Sands, J. (2008). Risk Management and Ethical Environment: Effects on Internal Audit and Accounting Control Procedures. *Journal of Applied Management Accounting Research*, 6(1).
- Rao, A. (2007). Evaluation of Enterprise Risk Management (ERM) in Dubai: An Emerging Economy. *Risk Management*, 9(3), 167–187. doi:10.2307/4500411
- Risk and Insurance Management Society. (2011). *2011 Enterprise Risk Management Survey*. Retrieved April 21, 2013, from <http://www.rims.org/resources/erm/Pages/default.aspx>
- Sarens & Christopher, (2010). The association between corporate governance guidelines and risk management and internal control practices: Evidence from a comparative study. *Managerial Auditing Journal*, 25(4), 288-308. doi 10.1108/02686901011034144
- Saunders, M. and Lewis, P. (2012). *Doing Research in Business and Management*. United Kingdom: Pearson Education.
- Securities and Exchange Commission (2009). *Study of the Sarbanes Oxley Act of 2002 Section 404 Internal Control over Financial Reporting Requirements*. Retrieved from http://www.sec.gov/news/studies/2009/sox-404_study.pdf

- Selto, F., & Widener, S. (2004). New directions in management accounting research: Insight from practice. *Advances in Management Accounting*, 12, 1–35.
- Selznick, P. (1996). Institutionalism “old” and “new”. *Administrative Science Quarterly*, 41(2), 270-277.
- Shenkir, W. G., & Walker, P. L. (2011). Enterprise Risk Management: Frameworks, Elements, and Integration. *Institute of Management Accountant*, 1-29. Retrieved August 24, 2013, from http://www.imanet.org/PDFs/Public/Research/SMA/ERM_Frameworks,%20Elements,%20and%20Integration.pdf
- Shenkir, W. G. & Walker, P. L. (2006). Enterprise risk management and the strategy risk- focused organisations. *Cost Management*, 20(3), 32-38.
- Vecchiato, P., & Secombe, A. (2013, May, 29). Doubts over promise of ‘rescue plan’ for battling mine sector. *Business Day Live*. Retrieved August 24, 2013, from <http://www.bdlive.co.za/business/mining/2013/05/29/doubts-over-promise-of-rescue-plan-for-battling-mine-sector>
- Vijayakumar, A., & Nagaraja, N. (2012). Internal control systems: effectiveness of internal audit in risk management at public sector enterprises. *BVIMR Management Edge*, 5(1), 1–8.
- Yin, R. K. (2003). *Case Study Research: Design and Methods*. Thousand Oaks: Sage Publications.

APPENDIX 1: TYPICAL RISKS FACING MINING INDUSTRY

Table 6: The 12 most cited risks (in no particular order)

Risk type	Explanation
Increased regulation and changes in government policy	Compliance with various corporate and government regulations, e.g. resource nationalism, the Mining Charter's current compliance requirements which have a potential to change, compliance with Health and safety regulations
Health and safety risk	The most important one because mining is dangerous firstly, so you want to prevent people from getting hurt or die. Health and hygiene risk because of the environment you work in: there is dust, there is noise, there is heat exposure. You want to ensure that people remain healthy
Environmental risk	Mining operations rely on other external resources availability for their operations such as power shortage risk and water supply shortage risk. Mining operations also have a big impact on the environment and e.g. water pollution they make
Financial risk	Financial risk relates to aspects of cost, revenue, commodity price fluctuations,
Market risk	It is more external market events, the market that mines are supplying their products to, which also may have impact on company financials
Socio economic and community type risk	The biggest headline risk for all mining companies. Includes industrial action risk and how to prevent that or stop from escalating. Potential land disputes that may arise between mining companies and local communities. The lack of service delivery by local governments, the use of housing benefits for other purposes and the seeming inability of stakeholders to agree on social upliftment projects causes raised expectations from the communities irrespective of the "limited resources" mines may have.
Capital project execution	Mining projects comprise a significant percentage of company spend and require particular focus on budgets, schedules and execution particularly due to scarcity of inputs

Risk type	Explanation
	therefore if not managed properly they can be the cause of dramatic losses in project value.
Reputational risk	Assessing and monitoring and preventing/minimising any events that could harm the company's reputation.
Political risk	Political risk in various countries the mines operate in as well the upcoming elections in RSA
Workforce strike risk	Workforce strikes/industrial action due to labour disputes and has an impact on all the other disciplines – production, finance, etc. It can potentially break the company
Skills shortage	Skills shortages apparent in most countries and South Africa, amidst unemployment – e.g. laying off staff has a consequence effect of losing staff that companies want to keep, resulting in losing both.
Long term business strategy	Risks related to company strategy and sustainability of the business, touching on most of the risks above.

APPENDIX 2: LETTER OF CONSENT

INFORMED CONSENT

The impact of Enterprise Risk Management (ERM) on an organisation's internal control system

I am conducting research on Enterprise Risk Management (ERM), and am trying to find out more about how ERM enhances an organisation's internal control system. Our interview is expected to last about an hour and half, and will contribute to our efforts seeking to understand, assess and explain the impact ERM has on the internal control system of an organisation. **Your participation is voluntary and you can withdraw at any time.** All data will be kept confidential.

If you have any concerns, please contact me or my supervisor. Our details are provided below.

Researcher name: Thelma Kganakga

Email: thelma.kganakga@ubank.co.za

Phone: 0844608823

Research Supervisor Name: Ross Liston

Email: ross.liston@gmail.com

Phone: 0828525913

Signature of participant: _____

Date: _____

Signature of researcher: _____

Date: _____

APPENDIX 3: SEMI-STRUCTURED INTERVIEW GUIDE

THE IMPACT OF ENTERPRISE RISK MANAGEMENT (ERM) ON AN ORGANISATION'S INTERNAL CONTROL SYSTEM

- Thank the person for attending
- Explain purpose of research and interview, emphasising that it is participant's own opinions that are important
- Explain the use of recording facility to ensure important information that will be shared is not omitted.
- Ask if willing to be interviewed and stress this is their decision.
- If willing, ask them to sign the consent form; if not, thank them for their time and close the interview.

Interviews will be held with the following participants:

- Chief Risk Officer or equivalent and some of their team members
- Member(s) of the board
- Internal audit Head

Interview

Research themes

The main themes we will discuss are the context of your organisation in relation to its size and culture; ERM as a business imperative; impact of ERM on internal control; and key factors essential to ensure that the implemented ERM enhances the internal control system.

Questioning technique

There are main questions under each theme with sub-questions. These sub-questions will be used throughout the interview depending on whether the response given requires further probing, follow up or clarity.

CHIEF RISK OFFICER

1. Organisation context

- 1.1 Are you using a formal enterprise risk management (ERM) framework within your organisation?
 - *Follow up:* When did you start adopting this framework?
- 1.2 What is the total number of full-time employees in your organisation?
 - *Follow up:* Does the size of your organisation affect your ERM interventions?
 - *Probe:* How?
- 1.3 How would you describe the culture of your organisation? (*Provide clarity as culture can be understood in many ways - i.e. whether the culture is mechanistic/organic; centralised/ decentralised; change averse or risk aware*)
 - *Follow up:* How has it impacted your risk management and internal controls management?
 - *Probe:* Please expand a bit more on this aspect?

2. ERM as a business imperative

- 2.1 Why did you decide to adopt ERM?
- 2.2 Does the company have clear objectives that have been communicated so as to provide effective direction to employees on risk management and control issues?
 - *Follow up:* Do those objectives and related plans include measurable performance targets and indicators for employees?
 - *Probe:* Why do you do it that way?
- 2.3 To what extent does the board formally discuss top risk exposures facing the organisation when they discuss the organisation's strategic plan?
- 2.4 What types of risks are crucial for your business?
 - *Follow up:* How often are the risks assessed?
 - *Follow up:* Are those risks industry-wide or specific to your organisation?
- 2.5 Is there risk and control ownership at Exco level? I.e. Do you assign ownership of risk and controls to every Exco member?
 - *Probe:* Why?
- 2.6 Is there a clear understanding by management and others within the company of what risks are acceptable to the Board? I.e. the risks and their tolerance levels?
- 2.7 What is your view on having a resourced risk management function in an organisation?
 - *Probe:* Could you please explain that a little more for me?
- 2.8 What tool(s) are you using to record and track your risks?
 - *Probe:* Why did you decide to use those tool(s)?

3. Impact of ERM on internal control

- 3.1 How do you see the relationship between risk and internal control?
- 3.2 What is the importance of internal control to your business?

- *Clarify understanding:* So what you are saying is...?
- 3.3 How do you design or develop internal controls within your company?
- 3.4 Prior to implementing ERM, how did your organisation define internal controls?
- *Probe:* How did you find that?
- 3.5 Has implementing ERM enhanced your internal control system?
- *Probe:* If so, what specific improvements have you seen or experienced?
- 3.6 What mechanisms do you use to track and monitor internal control improvements?
- 3.7 What is the ultimate goal of having an effective internal control?

4. Key factors to ensure ERM enhances internal control system

- 4.1 Since the implementation of ERM, what have you seen as the key factors that contributed to success (or challenges) you are experiencing with how you manage your internal control system?
- *Clarify understanding:* What you are saying is...?
- 4.2 What advice can you give to companies implementing ERM?
- *Clarify understanding:* To make sure I understand you correctly, you believe that....?

INTERNAL AUDIT

1. Organisation context

- 1.1 Are you using a formal enterprise risk management (ERM) framework within your organisation?
- *Follow up:* When did you start adopting this framework?
- 1.2 What is the total number of full-time employees in your organisation?
- *Follow up:* Does the size of your organisation affect your ERM interventions?
 - *Probe:* How?
- 1.3 How would you describe the culture of your organisation? (*Provide clarity as culture can be understood in many ways - i.e. whether the culture is mechanistic/organic; centralised/ decentralised; change averse or risk aware*)
- *Follow up:* How has it impacted your risk management and internal controls management?

2. ERM as a business imperative

- 2.1 To what extent does internal audit evaluate whether ERM framework followed meets organisational needs and regulatory expectations?

3. Impact of ERM on internal control

3.1 Where does internal audit provide assurance – is it on effectiveness of all controls or effectiveness of controls in key business processes or on key risks identified by the organisation?

- *Probe:* Could you perhaps give me a bit more detail/ examples about your response?

3.2 Has ERM enhanced how you provide assurance on the effectiveness of the controls?

- *Probe:* How - Please can you elaborate a little more on your thoughts about this?

3.3 How does your control environment look since you have implemented ERM?

3.4 How do you see the relationship between risk, internal control and assurance?

4. Key factors to ensure ERM enhances internal control system

4.1 In your experience, what are the key factors in ensuring that enterprise risk management enhances an organisation's internal control system, if it does at all?

BOARD MEMBER

1. Organisation context

1.1 Are you using a formal enterprise risk management (ERM) framework within your organisation?

- *Follow up:* When did you start adopting this framework?

1.2 What is the total number of full-time employees in your organisation?

- *Follow up:* Does the size of your organisation affect your ERM interventions?
- *Probe:* How?

1.3 How would you describe the culture of your organisation? (*Provide clarity as culture can be understood in many ways - i.e. whether the culture is mechanistic/organic; centralised/ decentralised; change averse or risk aware*)

- *Follow up:* How has it impacted your risk management and internal controls management?

2. ERM as a business imperative

2.1 Why did you decide to adopt ERM?

2.2 Is there a clear understanding by management and others within the company of what risks are acceptable to the Board? I.e. the risks and their tolerance levels?

2.3 Is there risk and control ownership at Exco level? i.e. Do you assign ownership of risk and controls to every Exco member?

- *Probe:* Why do you do that?

2.4 Does the board formally discuss top risk exposures facing the organisation when you discuss the organisation's strategic plan?

2.5 What types of risks are crucial for your business?

- *Follow up:* How often are the risks assessed?

- *Follow up: Are those risks industry-wide or specific to your organisation?*

2.6 What is your view on having a resourced risk management function in an organisation?

- *Clarify understanding: So what you are saying is....?*

3. Impact of ERM on internal control

3.1 How do you see the relationship between risk and internal control?

3.2 What is the importance of internal control to your business?

3.3 How do you develop internal controls within your company?

- *Probe: Could you perhaps give me a bit more detail on this?*

3.4 Prior to implementing ERM, how did your organisation define internal controls?

- *Probe: How did you find that?*

3.5 Has implementing ERM enhanced your internal control system?

- *Probe: If so, what specific improvements have you seen?*
- *Follow up: How does your control environment look now since you have implemented ERM?*

3.6 What mechanisms do you use to track and monitor internal control improvements?

3.7 Does it matter to the board if the organisation has an effective internal control system?

4. Key factors to ensure ERM enhances internal control system

2.1 Since embarking on the ERM journey, what would you say are the key factors that contributed to success (or challenges) you are experiencing with how your Exco and management are managing your internal control system?

2.2 What advice can you give to companies implementing ERM?

- *Clarify understanding: To make sure I understand you correctly, you believe that...?*

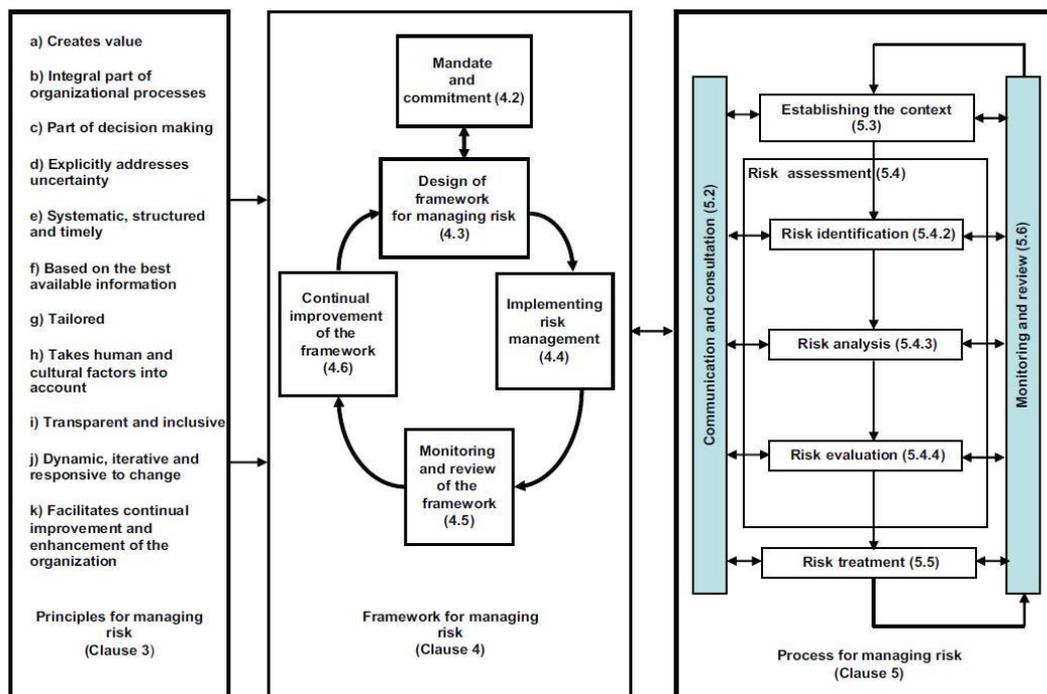
APPENDIX 4: HIGH-LEVEL OVERVIEW OF TWO OF THE WIDELY USED ERM STANDARDS AND GUIDELINES

A summary overview of the ISO 31000: 2009 Risk Management - Principles and Guidelines and the COSO: 2004 Enterprise Risk Management - Integrated Framework is provided in Table 7, with summary process diagrams in Figure 7 and Figure 8.

Table 7: High-level overview of the ISO 31000 and COSO 2004

	ISO 31000	COSO Framework
Who it applies to	All industries and sectors	Companies interested in satisfying internal control needs and in moving to a fuller risk management process
Its primary objective	Organisational, may be used for certification or regulatory compliance	Organisational, Compliance and Control
The type of document	Internationally recognised Standard as an established norm or requirement	Guidance document or framework

Figure 7: ISO 31000 Risk Management Guideline



Source: ISO 31000 (2009)

The ISO risk management process is used to implement coordinated activities and consists of the systematic application of principles, policies, procedures and practices for risk identification, analysis, evaluation and treatment tasks. It also includes aspects of communication, establishment, consulting, monitoring and risk review. The principles on the left guide the creation of the framework. The framework then defines the process. The performance of the process feeds back into the framework.

Figure 8: COSO: 2004 Enterprise Risk Management Framework



The multi-dimensional nature of ERM is represented by the COSO cube (COSO 2004). The front section of the cube represents the generic risk management process. The top section of the cube represents four generic business functions applicable to any organisation, and under which the objectives of the organisation may be classified (Strategic, Operations, Reporting, and Compliance). The side area of the cube represents the hierarchical division of the enterprise into its various operating units. The cube therefore represents the application of the risk management process across the functional areas of the business, and its integration throughout the enterprise, top to bottom.