THE DEVELOPMENT OF AN ENTERPRISE-WIDE RISK MANAGEMENT FRAMEWORK IN AN ORGANISATION

A Louw, B Com (Accounting)

Mini-dissertation submitted in partial fulfilment of the requirements for the degree ***Masters in Business Administration (MBA)*** at the Vanderbijlpark campus of the North-West University

Supervisor: Prof Jan du Plessis

November 2007

Abstract

Enterprise-wide risk management (ERM) has over the past few years emerged as a widespread practice in organisations. It has been increasingly included in regulatory, corporate governance and organisational management blueprints. Making sense of all these developments is a big challenge. Contributing to this difficulty is today's challenging global economy, business opportunities and risks that are constantly changing. There is a constant need for identifying, assessing, managing and monitoring the organisation's business opportunities and risks in order for organisations to succeed.

Risk management is a well-established philosophy; however, organisations are struggling to implement, embed and sustain a pragmatic ERM solution that is robust, adds value and creates a balance between cost and reward. In surveys done it was noted that ninety percent of executives are building or want to build an enterprise risk management process into their organisations, but only eleven percent report they have completed the implementation successfully. The question raised is thus, if ERM is widely known and executives are eager to build an ERM process into their organisations, why is ERM not successfully implemented, embedded and monitored in order to give the assurance to senior executives and all other stakeholders that all potentially significant business risks are identified and managed.

In this study a practical nine-step ERM process is derived from various case studies and other information from publications, journals, and articles. Key learnings from successful ERM implementations are also highlighted in order to assist other organisations to successfully implement, embed, and sustain a pragmatic and dynamic ERM process that enables better informed decisions, greater management consensus and increased management accountability.

From all the case studies and other relevant information researched it is evident that every organisation follows different steps and phases to get to their ERM solution. No 'one size fits all' solution exists. A cookbook recipe for implementing ERM is not feasible as so much depends on the culture of

the organisation and the change agents who lead the effort. The implementation of any new ERM process will have some or other disruptive effect due to the change management aspects.

It is important to understand that the ERM process is a journey with no finite end. It is an interactive process and needs commitment from top management to succeed. All the organisations that have successfully implemented ERM had one common belief with regard to the implementation of ERM. They believed that ERM was creating, protecting and enhancing value by managing ERM.

The key lessons learnt from the study are summarised in Key Success Factors (KSF) that are recommended for value adding ERM through effective implementation, embedding, monitoring and assurance over ERM.

The successful implementation of ERM is not an easy task, but it is no longer a "nice to have". In today's challenging global economy, business opportunities and risks are constantly changing and therefore a dynamic and robust ERM process should be implemented to ensure effective management of risks. As proven the mismanagement of risks can carry an enormous price.

Acknowledgements

I would like to express my sincere gratitude to the following people for their constructive inputs and, without whom this research would not have been possible:

- Professor Jan du Plessis for his personal commitment and effort, and professional guidance.
- My family and friends who supported me in many practical ways and never stopped believing in me.
- God, for giving me the opportunity and strength to complete this study.

List of Acronyms

CAE	—	Chief Audit Executive
CEO	—	Chief Executive Officer
CFO	—	Chief Financial Officer
CLO	—	Chief Legal Officer
CRO	—	Chief Risk Officer
CSF	—	*Critical Success Factors*
EAR	—	Earnings at risk
ERA	—	Enterprise Risk Assessment
ERM	—	Enterprise-wide Risk Management
KRI	—	Key Risk Indicators
NYSE	—	New York Stock Exchange
SVA	—	Shareholder value-added
VAR	—	Value at Risk

List of Institutes

FERMA	—	Federation of European Risk Management Associations
IIA	—	Institute of Internal Auditors
IRMSA	—	Institute of Risk Management South Africa

TABLE OF CONTENTS

List of Tables

CHAPTER 1
NATURE AND SCOPE OF THE STUDY

1.1 INTRODUCTION

Valsamakis, Vivian and Du Toit (2005:12) define risk management as a managerial function aimed at protecting the organisation, its people, assets, and profits against the physical and financial consequences of risk. It involves planning, coordinating and directing the risk control and the risk financing activities in the organisation.

The ever-changing economy and business environment, for example e-commerce, technology, internet democracy and others, result in uncertainties in today's economy. Every organisation is, to some extent, in the business of risk management, irrespective of what products or services the organisation delivers. In the modern age no organisation can do business without taking risk. In today's challenging global economy, business opportunities and risks are constantly changing. There is a constant need for identifying, assessing, managing and monitoring the organisation's business opportunities and risks. The mismanagement of risk can carry an enormous price (Barton, Shenkir & Walker, 2002).

Levitt, former chairperson of the U.S. Securities Exchange Commission rightly said that the average organisation of today is a complex enterprise engulfed by rapid technological change and fierce global competition. It is essential that risk be assessed on an ever-changing landscape as most major losses are as the result of a series of high impact but low likelihood events (Shough 2006:17).

Stewart (2002:202) adds to the above by saying that risk is good and the point of risk management is not to eliminate all risks, because that would also eliminate reward. The point is to manage risk by choosing where to place bets, and where to avoid betting altogether.

The King Report on Corporate Governance for South Africa – 2002, referred to as the King II Report (2002:73), highlights the importance of a thorough understanding of the risks of the organisation in the pursuance of its objectives, together with the strategies employed to mitigate those risks. This is thus essential for a proper appreciation of a company's affairs by the board and stakeholders. This report also recommends enterprise-wide risk management strategies for all organisations, because risk management is a holistic way to design, implement and manage capabilities for managing an organisation against risks that matters, and to identify and plan for opportunities. This strategy includes, but is not limited to the following risks: strategic risk, financial risk, security risk, information technology risk, business continuity, operational risk, human resources risk, compliance risk, and safety, health and environment risk.

Dickinson (2001:360) asserts that enterprise-wide risk management (ERM) has emerged as a concept and as a management function within organisations since the mid-1990s. ERM is a systematic and integrated approach to the management of the total risks that an organisation faces. Its emergence can be traced to two main causes. Firstly, as a result of high profile organisation failures and preventable large losses, and secondly, due to shareholder value models playing a greater role in strategic planning.

ERM became a prerequisite for successful and well-managed businesses. Over time, a business that cannot manage its key risks effectively will simply disappear.

This chapter contains the problem statement and a discussion of the research objectives, in which the objectives are set out. The research methodology and the division of chapters are explained.

1.2 PROBLEM STATEMENT

In today's challenging global economy, business opportunities and risks are constantly changing. There is a constant need for identifying, assessing, managing and monitoring the organisation's business opportunities and risks.

Risk management is a well-established philosophy; however, organisations are struggling to implement, embed and sustain a pragmatic ERM solution that is robust, adds value and creates a balance between cost and reward.

According to the results of the 1995 risk management study conducted by Arthur Andersen (1995), less than 50 percent of senior executives are satisfied that their existing risk management systems are able to identify and manage all potentially significant risks and more than 50 percent of participants have made recent significant changes to their existing risk management processes. Furthermore, nearly 60 percent are planning significant changes within the next few years.

The U.S. Protiviti Risk Barometer (Protiviti, 2007) notes that almost fifty percent of senior executives surveyed, lack a high degree of confidence that their current risk management capabilities allow them to properly identify and manage all potentially significant business risks.

As noted in the Best's Review (2005:115), a survey of risk management executives was done which found 90 percent of these executives are building or want to build an enterprise risk management process into their organisations, but only 11 percent report they have completed the implementation. This survey found that companies who have already implemented ERM have a higher "level of value" than those who have not yet fully implemented ERM. The top three benefits derived from this study are better-informed decisions, greater management consensus and increased management accountability.

The question raised is if ERM is widely known and executives are eager to build an ERM process into their organisations, ***why is ERM not successfully implemented, embedded and monitored in order to give the assurance to senior executives and all other stakeholders that all potentially significant business risks are identified and managed***.

1.3 RESEARCH OBJECTIVE

The objective of this study is to identify key learnings from successful ERM implementations in risk management that could potentially be useful to other organisations in developing and expanding on existing ERM practices to facilitate the preparation and practical implementation of ERM in order to give assurance to all stakeholders that all potentially significant risks are identified and managed.

1.4 RESEARCH METHODOLOGY

The research method involves an extended literature review.

1.4.1 Literature review

The research focuses on actual case studies by other researchers on the ERM topic. Additional relevant information has been obtained from various publications such as textbooks, journals, presentations and previous studies on the subject. An ERM process was developed and key learnings to enhance the development of an effective ERM process were compiled.

1.4.2 Research design

Due to the exploratory nature of this study, hypotheses will not be formulated.

1.5 LIMITATIONS OF THE STUDY

The research is intended to identify a practical ERM process and not to deduce one ERM process or framework that fits all organisations.

1.6 DIVISION OF CHAPTERS

The study will be divided into four chapters. In Chapter 1 the nature and scope of the study are presented which include the problem statement, research objectives, method and procedures. In Chapter 2 the enterprise-wide risk management process is discussed. Subsequently, in Chapter 3 the results of the study, inclusive of the devised ERM process and most important key learnings from this study are discussed and in Chapter 4 the conclusions and recommendations are presented.

CHAPTER 2
ENTERPRISE-WIDE RISK MANAGEMENT

2.1 INTRODUCTION

During most of history, mankind has had no more than a gut feel when faced with uncertainty. This, however, changed dramatically in the 1600s when mathematics was applied for the first time in games of change. The discoveries that followed gave solid foundations to the insurance industry and catalysed the development of the field of risk management. Business could finally make rational assessments and develop suitable plans to manage unacceptable levels of risk (Bernstein, 1998).

The ever-changing economy and business environment, for example e-commerce, technology, internet democracy and others, result in uncertainties in today's economy. Every organisation is, to some extent, in the business of risk management, irrespective of what products or services they deliver. In the modern age no organisation can do business without taking risk. In today's challenging global economy, business opportunities and risks are constantly changing. There is a constant need for identifying, assessing, managing and monitoring the organisation's business opportunities and risks. The mismanagement of risk can carry an enormous price (Barton, Shenkir & Walker, 2002).

Dickinson (2001:360) states that ERM has emerged as a concept and as a management function within organisations since the mid-1990s. ERM is a systematic and integrated approach designed to manage the total risks that an organisation faces. Its emergence can be traced to two main causes. Firstly as a result of high profile company failures and preventable large losses, and secondly, due to shareholder value models playing a greater role in strategic planning.

As noted in the Best's Review (2005:115), a survey of risk management executives was done which found that 90 percent of executives are building or want to build an enterprise risk management process into their organisations, but only 11 percent report they have completed the implementation. The survey by the Conference Board/Mercer Oliver Wyman, found that companies who have already implemented ERM have a higher "level of value" than those who have not yet fully implemented ERM. The top three benefits derived from this study are better-informed decisions, greater management consensus and increased management accountability.

2.2 DEFINING RISK

Risk is a general term and different disciplines define and interpret risk differently. Irrespective of the discipline where risk is used, risk is normally associated with either an opportunity or a danger (Puschaver & Eccles, 1998:3).

According to the Deloitte Risk Intelligence Series (2006:3), risk is the potential for loss or the diminished opportunity for gain caused by factors that can adversely affect the achievement of an organisation's objectives. Organisations that focus solely on risk avoidance may survive but rarely thrive; only those that intelligently manage risk taking as a means to value preservation and value creating will excel in today's risky yet opportunity–rich business environment.

Valsamakis, Vivian and Du Toit (2005:29) define risk as a deviation from the expected value. It implies the presence of uncertainty. There may be uncertainty as to the occurrence of an event producing a loss, and uncertainty as regards the outcome of the event. The degree of risk is interpreted with reference to the degree of variability and not with reference to the probability that it will display a particular outcome. The standard deviation becomes a good measure of risk.

According to Barton *et al.* (2002), 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."

Shough from Deloitte (2006:1) defines risk as an uncertain future event that could influence the achievement of an organisation's objectives. These could include strategic, business, operational, process, people, financial and compliance risks, amongst others.

The level of knowledge and insight with regard to a situation determine the decision maker's level of self-confidence and security. The more insecure the decision maker is with regard to the likelihood of events and the impact thereof, the greater the risk (Valsamakis *et al.*, 2003:31-32). The severity of the risk can thus be interpreted in terms of the frequency of the event and the likelihood of a specific outcome (Cronje, De Swardt, Malobola, De Beer, Mutezo & Botha, 2004:11).

Risk further encompasses the uncertainty of future reward in terms of both the upside and downside. And opportunity in business arises from managing the future. Companies today must face and manage the future knowing that they cannot simply carry on with business as usual (Barton *et al.*, 2002:81).

Different types and classification of risks exist, which includes both internal and external risks. Some examples are strategic and execution risks, value-based risk, information-based risk, environmental risks, business process-based risks, people based risks, compliance risk, asset risk, governance risk, infrastructure risk, competitive risk, security risk, privacy risk, business continuity, reporting risk, and financial risk (Protiviti, 2006:54).

Possible sources of risks may include business interruption, commercial/legal relationships, custody of information, financial or market, management activities and controls, natural events, occupational health and safety, political, property and assets, human resource behaviour,

public/professional/product liability, security, socio-economic, technology, technical, and operations (Protiviti, 2006:54).

All organisations are not exposed to the same risks and therefore different organisations focus on different risks than others (Cronje *et al.*, 2004:31).

2.3 IMPORTANCE OF A RISK LANGUAGE

In Genesis 11:6 in the Holy Bible the Lord said, "If as one people speaking the same language they have began to do this, then nothing they plan to do will be impossible for them".

This illustrates the importance of a common language. In the previous section the definitions of risk were set out. These definitions are the starting point of a common risk management language that should be communicated and entrenched into the daily risk management operations (De la Rosa, 2003:152).

Espersen (2007:69) states that it is important that a risk language is created for every organisation as part of their ERM efforts. The author adds that the language ensures that everyone throughout the organisation shares a common method of speaking about risk. In addition, the author also gives reasons for having a risk language for every organisation. Firstly, as everyone in the organisation has a role in effective risk management, an organisation needs a risk language to enhance its risk culture. Secondly, a common language is needed to cut through different layers and break down silos within the organisation. Thirdly, without a common risk language, the risk management team can get "lost in translation" by spending too much time resolving communication issues at the expense of the team's primary responsibilities. Lastly, having a common risk language contributes in internal audit process improvement as both the client and the auditor understand the meaning of risk.

2.4 DEFINING RISK MANAGEMENT

Various authors define risk management as follows:

Risk management is defined as a field of activity seeking to eliminate, reduce and generally control pure risks (such as fraud, safety and fire) and to enhance the benefits and avoid detriment from speculative risks (such as financial investment and marketing) (Waring & Glendon, 2001:3).

Sawyer, Dittenhofer and Scheiner (2003:1388) define risk management as a process designed to identify, manage, and control potential events to provide reasonable assurance regarding the achievement of the organisation's objectives.

Further risk management is defined as a general management function that seeks to assess and address the causes and effects of uncertainty and risk in an organisation. The purpose of risk management is to enable an organisation to progress towards its goals and objectives in the most direct, efficient and effective way (University of Surrey – Risk Management, 2005).

The definitions above describe risk management as a systematic and thorough business discipline which Valsamakis *et al.* (2005:2) see as a modern development in risk management.

Sesel (2000:1) concurs that modern risk management is accepted as a means of protecting the bottom line and assuring long-term performance. It has become a universal management process involving quality of thought, quality of process, and quality of action. Thus risk management today should form part of the management function in every organisation

2.5 THE IMPORTANCE OF RISK MANAGEMENT

Valsamakis *et al.* (2005:7) state that the reasons for the management of risks are directly linked to the corporate objectives of the organisation, which are survival, growth, and maximisation of shareholder value and profits. Linked to that, Cohen and Peacock (1998:11) note that taking and managing risk is at the heart of shareholder value creation.

Therefore adopting a risk management program, which reduces risk, is of itself consistent with the general reason for the existence of a firm. It is not surprising that the adoption of a risk management program features in most codes on corporate governance (Valsamakis *et al.*, 2005:7).

Drucker (in Valsamakis *et al.*, 2003:12) emphasises the importance of risk management in an organisation by highlighting that risk management may be as important as entrepreneurship and business acumen in propelling the economic growth of the western world.

Although no one can predict the future, there are vital issues that demand serious attention and the common threat is the management of risk (Arminas 2003:1).

Sammer (2001:1) summarises the importance of risk management by saying that the effective management of risks is becoming a critical driver in many organisations' success or failure.

2.6 THE ROLE OF CORPORATE GOVERNANCE IN RISK MANAGEMENT

Large corporate scandals and failures from Enron, Worldcom and others during 2001 and 2002, resulted that shareholders lack confidence in companies and corporate governance. The ethical behaviour of directors and poor corporate governance are directly blamed for these failures (Ulick, 2002:1-5). These events directly contributed to the greater focus on corporate governance in the business environment. Various policies, corporate codes and acts were published as a result of the above and include firstly the King II Report in 2002, which consists of six focus areas namely: board of directors, risk management, internal audit, integrated sustainable reporting, accounting and auditing and compliance and execution. Secondly in 2002, after the Enron debacle, the Sarbanes-Oxley Act was enforced. This act stipulates requirements with regard to corporate compliance and auditing (Gray & Manson, 2005:91). Thirdly, in January 2003 Britain published the Higgs Report. In this report certain changes were made to the "Combined Code" that was released in 1999 by the Turnbull Committee. The Higgs Report also gives guidelines with regard to corporate governance to non-executive directors of companies (Gray & Manson, 2005:607).

According to Valsamakis *et al.* (2005:73), all the above guidelines and policies were compiled with a mutual objective to explain principles that directors and management must adhere to in order to manage organisations to the benefit of all shareholders and stakeholders.

According to The King II report (2002:17), corporate governance is concerned with holding the balance between economic and social goals and between individual and communal goals. The aim is to align as nearly as possible the interests of individuals, corporations and society.

The King II report is seen as the most important document with regard to corporate governance in South Africa. Therefore, the impact thereof is discussed in the following section.

2.7 THE KING II REPORT

Cronje *et al.* (2004: 51) stated that investors are willing to pay a premium for good control and corporate governance. Investors believe that organisations with sound corporate governance will have sustainable performance with an increase in share prices. Corporate governance is a method to keep risk low by either risk evasion or proper internal control. The focus on corporate governance is a tendency and no organisation want to stay behind.

The most important principles as described in the King II report are as follows and are used as basis for the IRMSA Code of Practice (King II Report, 2002: 74 – 91):

- *Principle 1 – Board accountability for enterprise risk management.* This principle refers to Section 2, Chapter 2 paragraph 1 of the King II report that states "The total process of risk management which includes a related system of internal controls is the responsibility of the board".
- *Principle 2 – A framework of enterprise risk management.* This principle refers to Section 2, Chapter 1, paragraph 11 of the King II report which states, "Sound risk management and internal control frameworks, tailored to the specific circumstances of the company, should be part of the daily operational activities of a company, and should not be viewed independently of normal business activities".
- *Principle 3 – Organisational structures for enterprise risk management.* This principle refers to Section 2, Chapter 2, paragraph 1 and states, "Management is accountable to the board for designing, implementing and monitoring the process of risk management, and integrating it into the day-to-day activities of the company".
- *Principle 4 – A structured process of risk assessment.* This principle refers to Section 2, Chapter 3, paragraph 1.2 and states, "The risk assessment process should consider risks that are significant to the achievement of the company's objectives".
- *Principle 5 – A risk-based control environment.* This principle refers to Section 2, Chapter 3, paragraph 1 and states, "Controls should be established to encompass all management responses to risk".

- *Principle 6 – A system of risk monitoring.* This principle refers to Section 2, Chapter 3, paragraph 1.5 and states, "The monitoring of risks should be linked to key performance indicators and organisational objectives, so that the accuracy of the risk assessment and the effectiveness of internal controls can be evaluated objectively".
- *Principle 7 – A process of risk reporting.* This principle refers to Section 2, Chapter 4, paragraph 3 and states, "The reports from management to the board should provide a balanced assessment of the significant risks and the effectiveness of the system of internal control in managing those risks".
- *Principle 8 – Embedding the processes of enterprise risk management.* This principle refers to Section 2, Chapter 3, paragraph 1.3 and states, "These should be designed to respond to risks throughout the company and its external environment and should include a diverse range of activities aimed at enhancing the control environment".
- *Principle 9 – Assurance processes for key risks and for the risk management process.* This principle refers to Section 2, Chapter 3, paragraph 2 and states, "The system of risk management and internal control should, therefore, be intertwined with the company's operating activities to provide assurance that enterprise-wide policies and procedures are in place to address all forms of risk identified as inherent to the company's activities".
- *Principle 10 – Incorporating the risk-related aspects of integrated sustainability reporting into the enterprise risk management framework.* This principle refers to Section 4, Chapter 1, paragraph 2 and states, "Sustainability means that each enterprise must balance the need for long-term viability and prosperity - of the enterprise itself and the society and environment upon which it relies for its ability to generate economic value – with the requirement for short-term competitiveness and financial gain".

From the above it is clear that the King II report emphasises the integrated risk management function that includes all risks in the organisation. The process that will address this need is referred to as enterprise-wide risk management (ERM).

2.8 DEFINING ENTERPRISE-WIDE RISK MANAGEMENT

A standard definition of ERM remains elusive. The Sycip Gorres Velayo & Co (SGV) Bulletin (2004:2) states that risk management approaches were up to recent years, in general, implemented in fragments and that risks were managed in silos. Valsamakis *et al.* (2005:77) state that traditional risk management approaches cannot deal with a company's continually evolving risks and opportunities created by globalisation, advances in technology, and a greater reliance on intangible assets such as the knowledge of is people.

All the changes in the business environment require an integrated risk management approach. COSO (2004b:4) defines ERM as:

> *"a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives".*

According to COSO (2004b:17) ERM is an ongoing entity-wide process, effected by people at every level of an organisation. Furthermore, ERM is applied in strategy setting across the enterprise, at every level and unit, and includes taking an entity-level portfolio view of risk, designed to identify potential events affecting the entity and manage risk within its risk appetite. ERM is able to provide reasonable assurance to an entity's management and board and geared to the achievement of objectives in one or more separate but overlapping categories – it is a means to an end and not an end in itself.

ERM encompasses aligning risk appetite and strategy, enhancing risk response decisions, reducing operational surprises and losses, identifying and managing multiple and cross-enterprise risks, seizing opportunities and improved deployment of capital (COSO, 2004b:16-21).

According to de la Rosa (2004:10), ERM is an approach designed to identify potential events that affect the business and the managing of its risks to be within pre-approved risk appetites.

DeLoach (2005:3), Protiviti's Managing Director explains that under ERM, the focus is on integrating risk management with existing management processes, identifying future events that can have both positive and negative effects and evaluating effective strategies for managing the organisation's exposure to those future possible events. ERM transforms risk management to a proactive, continuous, value-based, broadly focussed and process-driven activity.

Hence the goal of the ERM initiative is to create, protect and enhance shareholder value by managing the uncertainties that could either negatively or positively influence achievement of the organisation's objectives (DeLoach, 2005:3).

According to the FERMA Risk Management standard (2003:3), risk management is increasingly recognised as being concerned with both positive and negative aspects of risk. Risk management forms the central part of any organisation's strategic management and is the process whereby organisations methodically address the risks attaching to their activities with the goal of achieving sustained benefit within each activity and across the portfolio of all activities. The focus of good risk management is the identification and treatment of these risks. Its objective is to add maximum sustainable value to all the activities of the organisation.

According to the Deloitte Risk Intelligence Series (2007:2), a risk intelligent enterprise has various characteristics, which includes risk management practices that encompass the entire business, creating connections between the so-called silos that often arise within large, mature, and/or diverse corporations.

A risk intelligent enterprise also comprises of risk management strategies that address the full spectrum of risks and risk assessment processes that augment the conventional emphasis on probability by placing significant weight on residual risk or vulnerability. Further characteristics include risk management approaches that do not solely consider single events, but also take into account risk scenarios and the interaction of multiple risks. Furthermore, it also includes risk management practices that are infused into the corporate culture, so that strategy and decision-making evolve out of the risk-informed process, instead of having risk considerations imposed after the fact (if at all) and. Another characteristic is a risk management philosophy that focuses not solely on risk avoidance, but also on risk-taking as a means to value creation (Deloitte, 2007:2).

In summary, a significant change within the risk management arena has taken place, which has been a shift away from the silo-based approach to an enterprise-wide approach. Rather than looking at sectional risk areas, such as market risk or operational risk, organisations are now looking at risk holistically and how it can be managed as a whole throughout the organisation (Laloux, 2004:44).

2.9 REASONS TO IMPLEMENT ENTERPRISE-WIDE RISK MANAGEMENT

ERM provides a company with the process it needs to become more anticipatory and effective at evaluating, embracing and managing the uncertainties it faces as it creates sustainable value for stakeholders. It helps an organisation manage its risks to protect and enhance enterprise value in three ways namely that it helps to establish sustainable competitive advantage, it optimises the cost of managing risk, and it helps management improve business performance (Deloach, 2005).

According to Deloitte in the article The Risk Intelligent Enterprise 'ERM done right' (2006:3), organisations that are most effective and efficient in managing risks to both existing assets and to future growth will, in the long run,

outperform those that are less so. Thus, companies make money by taking risks and lose money by failing to manage them.

Protiviti (2006:3–4) recognises six fundamental reasons for implementing ERM:

The first reason is that ERM reduces unacceptable performance variability. Few companies have a systematic process for anticipating new and emerging risks. Therefore, many companies often learn of critical risks too late or by accident, spawning the "fire fighting" and crisis management, which drain resources and create new vulnerabilities. ERM assists management with improving the consistency of operating performance by increasing the emphasis on reducing earnings volatility, avoiding earnings-related surprises, and managing key performance indicator shortfalls. ERM improves the management of increasing risk mitigation costs and the success rate of achieving business objectives.

The second reason is that ERM aligns and integrates varying views of risk management. There are many silos within organisations with a point of view on managing risk, e.g. treasury, insurable risk, information technology and within business units. Silo mentality inhibits efficient allocation of resources and management of common risks, enterprise wide.

The third reason is that ERM is building the confidence of the investment community and stakeholders. Institutional investors, rating agencies and regulators are focusing more on the importance of risk management in their assessments of companies. By increasing their transparency with regard to risks and risk management capabilities and improve the maturity of their capabilities around managing critical risks, management will be able to articulate more effectively how well they are handling existing and emerging industry issues.

The fourth reason is that ERM enhances corporate governance. ERM and corporate governance are inextricably linked. ERM strengthens board oversight, forces an assessment of existing senior management level

oversight structures, clarifies risk management roles and responsibilities, sets risk management authorities and boundaries and effectively communicates risk responses in support of key business objectives. All these activities support good corporate governance.

The fifth reason is that ERM successfully responds to a changing business environment. As the business environment continues to change and the pace of change accelerates, organisations must become better at identifying, prioritising and planning for risk. ERM assists management with evaluating the assumptions underling the existing business model, the effectiveness of the strategies around executing that model and the information available for decision making. ERM drives management to identify alternative future scenarios, evaluate the likelihood and severity of those scenarios, identify priority risks, and improve the organisation's capabilities around managing those risks.

The sixth reason is that ERM aligns strategy and corporate culture. ERM assists management in creating risk awareness and an open, positive culture with regard to risk and risk management.

Businesses are always facing a variety of risks especially in the current times where the pace of change and resulting consequences to a business seems to be greater than ever. Over time, a business that cannot manage its key risks effectively will simply disappear (Protiviti, 2006:14).

Some forces that create uncertainty in today's economy includes globalisation, which has increased exposure to international events; the need for increased efficiency, innovation and differentiation; volatility of markets which creates more exposure and, understanding and responding to customer needs that remains the key in this demanding era of increasingly focused niche markets (Protiviti, 2006:14).

Furthermore, financial reporting is a significant risk area as companies focus on the sustainability of their disclosure process and internal control structures. Outsourcing has also become very popular due to transferring of risk.

Additional forces includes technology and the Internet, free trade and investment worldwide, complex financial instruments, deregulation of key industries; changes in organisational structures resulting from downsizing, reengineering and mergers, high customer expectations for products and services, business interruption and continuation risk, and more and larger mergers (Protiviti, 2006:14).

Based on a risk management study performed by Deloitte (2005:1) on the 1000 largest global companies it was concluded that eighty percent of companies that suffer great losses in value were exposed to more than one type of risk. But organisations may fail to recognise and manage the relationships among different types of risk, such as strategic risk, which can often increase exposure to other risks, such as operational or financial risks. Therefore organisations need to implement an integrated risk management function to identify and manage interdependencies among all the risks facing the organisation.

In the article "Disarming the Value Killers" (Deloitte, 2005: 1) the authors rightly say that the cost to implement a risk management plan is always less than the costs involved if your business does not manage risk.

Current risk management programmes are often viewed as a negative science focusing only on the hazardous or downside elements of risk. Entrepreneurs are beginning to realise that managing risk is an effective means of generating sustainable stakeholder value (IFAC, 1999:3).

Poor management of risks can come at an unbearable price for organisations. Over the past few years, organisations have witnessed a number of risk debacles that had a severe impact such as financial losses, decreased share value, dismissal of senior executives and management, damaged reputations, and in extreme cases the closure of businesses (Barton *et al.*, 2002).

Therefore today's economy requires a shift from the old, more traditional risk paradigm that managed risk management as a fragmented, ad hoc and narrowly focussed approach to a more dynamic, integrated, continuous and broadly focused risk management and awareness approach on all levels of the organisation. Table 2.1 illustrates the key features of the risk management paradigms.

TABLE 2.1: KEY FEATURES OF THE NEW RISK MANAGEMENT PARADIGM

Old Paradigm	New Paradigm
▪ Fragmented – departmental/function manage risks independently; accounting, treasurer, internal audit primarily concerned.	▪ Integrated – risk management coordinated with senior-level oversight; everyone in the organisation views risk management as part of his or her job.
▪ Ad hoc – risk management done whenever managers believe need exists to do it.	▪ Continuous – risk management process is ongoing.
▪ Narrowly focussed – primarily insurable risk and financial risks.	▪ Broadly focused – all business risks and opportunities considered.

(Source: Economist Intelligence Unit, Managing Business Risks, (1995). A similar analysis is presented in DeLoach (2000))

2.10 BENEFITS OF IMPLEMENTING ENTERPRISE-WIDE RISK MANAGEMENT

Key benefits for integrated risk management includes the management of prioritised related risks and opportunities across functional and sector boundaries which enables rational risks to be taken from an informed and control basis, and allowing effective allocation of resources. Enhanced information is provided to support decision making, e.g. future strategic direction, project launch approval, and capital investment approval (Keele University, 2006:3-4).

Integrated risk management also reduces business losses and earnings volatility, e.g. achieving planned margins and recognising and driving out costs. Furthermore, it reduces blanket risk mitigation costs (such as insurance) by improving the focus on internal management of risks (Keele University, 2006:3-4).

According to Deloitte (2006:3), the competitive benefits of improved risk intelligence include improved ability to prevent, quickly detect, correct, and escalate critical risks. It also reduces the burden on business operations by standardising risk management principles and language; and it reduces cost of risk management by improved sharing of risk information and integration of existing risk management functions.

Integrated risk management is a means to improve strategic flexibility for both upside and downside scenarios, and it provides "comfort level" to the board and other stakeholders that the full range of risks are understood and managed (Deloitte, 2006:3).

According to the position statement of the Institute of Internal Auditors (2004b), the benefits of ERM includes greater likelihood of achieving the company objectives; consolidated reporting of disparate risks at board level; improved understanding of the key risks and their wider implications;

identification and sharing of cross business risks; greater management focus on the issues that really matter; fewer surprises and crises; more focus internally on doing the right things in the right way; increased likelihood of change initiatives being achieved; capability to take on greater risk for greater reward; and more informed risk-taking and decision-making.

Successful companies are good at managing silos of risk. Enterprise-wide risk management offers them more effective risk management at potentially lower costs (Barton *et al.*, 2002).

Finally, a company with a sound risk management process can only gain. Recent surveys all recognise that well-governed companies in emerging markets with a sound ERM system can demand an additional share premium between 10 percent and 30 percent (Laloux, 2004:44).

2.11 CURRENT STATISTICS ON MATURITY OF ENTERPRISE-WIDE RISK MANAGEMENT IN ORGANISATIONS

An article published in the Fortune on 2 October 2006 noted that a study of the S&P 500 companies showed that overall risk levels (in other words the total number of high risks) more than doubled between 1985 and 2006. In 1985, only 35 percent of the S&P 500 faced high risk and highly volatile long-term earnings growth. By 2006, that number had risen to 71 percent. During the same period, the number of companies enjoying low risk and volatility fell from 41 percent to 13 percent. This further emphasises the importance of a robust and a value adding ERM solution (Colvyn, 2006: 44).

2.12 THE ENTERPRISE-WIDE RISK MANAGEMENT PROCESS

ERM is a journey, meaning it is a growth process in which the organisation integrates risk management with strategy setting aimed at improving the effectiveness of its risk management capabilities over time. Management's challenge is to keep the entrepreneurial side and the control side of the enterprise in balance and to avoid letting either one of these two activities

gain a disproportionate degree of strength relative to the other (DeLoach, 2005).

Various case studies and other information from publications, journals, and articles on ERM were consulted in order to derive an effective ERM process.

2.12.1 Case studies

2.12.1.1 Chase Manhattan Corporation, E.I. du Pont de Nemours and Company, Microsoft Corporation, United Grain Growers Limited and Unocal Corporation

Barton *et al.* (2002) analysed the risk management practices of Chase Manhattan Corporation, E.I. du Pont de Nemours and Company, Microsoft Corporation, United Grain Growers Limited and Unocal Corporation. The case studies demonstrated, in as much detail as the companies would publicly share, how they manage risk. One common theme emerged and that is that each company believed it was creating, protecting, and enhancing value by managing enterprise-wide risks. These five organisations were at various stages of developing an ERM approach, but all were assessed according to the 7 steps below.

Step 1 is risk identification. Before an organisation starts to manage risks, it must know what risks to manage. Organisations should make a formal, dedicated effort to identify all the organisation's significant risks. Various risk identification methods and techniques exist such as scenario analysis and self-assessments to ensure a dynamic and continuous risk identification process. Risk identification sessions also include a risk-ranking component and are based on dollar effects, severity or impact. Both the likelihood and impact of the risk is assessed.

Step 2 is risk measurement, which can be as simple as ranking and prioritising risks. The most developed areas for risk measurement are in financial risks. However, some risks are just not measurable.

Step 3 involves the development of risk response strategies. Various combinations of risk response strategies are used, which includes avoidance, acceptance, transfer, and mitigation to manage risk. Decisions regarding risk response strategies should be dynamic and should be continuously re-evaluated.

Step 4 is risk integration. A portfolio of risks should be built in a form of a risk map, a list of risk or a model that highlights the organisation's assessment of risks. Thereafter best practices and tools should be integrated and risk information of the organisation should be used to look at enterprise-wide management of those risks.

Step 5 addresses the driving of risk awareness throughout the organisation. This entails the task of instilling risk awareness in a corporate culture focused on other objectives than just risk management.

Step 6 involves the implementation of risk infrastructure. This includes the composition and responsibility of the Risk Committee, CRO, and Internal audit amongst others.

Step 7 involves the assignment of responsibility to the champions of ERM. Adopting ERM is a major cultural change for a company and in order to succeed it needs the commitment from the highest levels of management.

2.12.1.2 Vodacom Group (Pty) Ltd

The following ERM process is followed by the Vodacom Group (Pty) Ltd (Meiring, 2006:1-15):

Step 1 involves the establishment of the context. The context defines the area and stakeholders of the area for which the risk assessment will be done in terms of the organisation. It also refers to establishing risk management's objectives, tolerance and limits for the organisation's areas with significant

risks. Clear goals and objectives are vital to success. Management aligns these goals and objectives with the overall business objectives, strategies and performance goals and communicates these throughout the organisation through written policies. ERM responsibilities, authorities and accountabilities are assigned to appropriate personnel from the highest levels of the organisation down.

Step 2 is risk identification and sets out to identify an organisation's exposure to uncertainty. Different methods such as workshops, questionnaires, and one-on-one interviews are used to assist with the risk identification programme.

Step 3 is risk assessment, which is divided into the analysis of risks and risk ranking and profile. Risks are analysed by combining estimates of consequences and probability. Risks are ranked and a risk profile is compiled based on the results of the risk analysis, which gives a significance rating to each risk and provides a tool for prioritising risk treatment efforts.

Step 4 entails the evaluation of risks and involves the comparison of estimated risks against criteria, which the organisation has established. Risk evaluation is used to make decisions about the significance of risks to the organisation and whether each specific risk should be accepted or treated.

Step 5 is risk reporting. Different levels within the organisation require different information from the ERM process. Internal (Board of directors, business unit management) and external (Stakeholders) reporting is done.

Step 6 involves the treatment of risk, which is the process of selecting and implementing measures to modify the risk, if not accepted. Risk treatment includes avoidance, transfer, diversity, additional controls or share risk.

Step 7 involves assigning and managing of risk. Accountability helps to ensure that ownership of the risk is recognised and the appropriate management resource allocated.

Step 8 entails the monitoring and review of the ERM process by all assurance providers. The moment that the profile reveals a specific critical risk area, the process recommences the identification, analysis, evaluation and ultimately the implementation for new risk solutions.

2.12.2 Publications, journals and articles

2.12.2.1 Risk management standard from Federation of European Risk Management Associates (Ferma)

Ferma (2003:5-14) proposed a seven-step ERM process:

Step 1 is defining the organisation's strategic objectives.

Step 2 is risk assessment, which is the overall process of risk analysis and risk evaluation.

Step 3 entails the risk analysis, which consists of risk identification, risk description and risk estimation monitoring. The result of the risk analysis process can be used to produce a risk profile, which gives a significance rating to each risk, and provides a tool for prioritising risk treatment efforts. This ranks each identified risk so as to give a view of the relative importance.

Risk identification sets out to identify an organisation's exposure to uncertainty. This requires an in-depth knowledge of the organisation and the market in which it operates, the legal, social, political and cultural environment in which it exists as well as the development of a sound understanding of its strategic and operations objectives, including factors critical to its success and the threats and opportunities related to the achievement of these objectives.

The objective of risk description is to display the identified risks in a structured format such as a table. The use of a well-designed structure is necessary to ensure comprehensive risk identification, description and assessment process. By considering the consequence and probability of each of the risks

set out in this table, it should be possible to prioritise the key risks that need to be analysed in more detail.

Risk estimation monitoring can be quantitative, semi-quantitative or qualitative in terms of the probability of occurrence and the possible consequence.

Step 4 is risk evaluation. When the risk analysis process has been completed, the estimated risks are compared against risk criteria, which the organisation has established. Risk evaluation is thus used to make decisions about the significance of risks to the organisation and whether each specific risk should be accepted or treated.

Step 5 involves risk treatment, which is the process of selecting and implementing measures to modify the risk. Risk treatment responses include risk avoidance, risk transfer, risk financing and risk control/mitigation.

Step 6 is risk reporting and communication. Reporting is done both internally and externally. Internally, reporting is done to different levels within an organisation, as they need different information from the ERM process. External reporting is done to stakeholders on a regular basis with regard to risk management policies and the effectiveness in achieving its objectives.

Step 7 entails the monitoring and review of the risk management process. Effective risk management requires a reporting and review structure to ensure that risks are effectively identified and assessed and that appropriate controls and responses are in place.

2.12.2.2 Journal of Industrial Technology

The following six-step risk management process (Meier, 2000:4) is recommended by Dr Ronald Meier, in the August 2000 issue of the Journal of Industrial Technology:

Step 1 is the determination of objectives, which entails the decision on precisely what it is that the organisation expects that the risk management program will do.

Step 2 is the identification of the risks and involves the identification of risks through various tools and techniques.

Step 3 involves the evaluation of the risks. After the risks have been identified, the risk manager must evaluate risks by measuring the potential size of the loss and the probability that it is likely to occur. The evaluation requires ranking of priorities as critical risks, or unimportant risks.

Step 4 entails the consideration of alternatives and selection of risk treatment. Risk treatment devices are used in deciding which techniques to use to deal with a given risk.

Step 5 implementation of the decision to retain or treat a specific risk. This decision is supported by policies and procedures to reduce or eliminate the probability of occurrence and the severity of the impact.

Step 6 involves the evaluation and review of the risk management program. Due to constant changes in the business environment, new risks arise and old ones might not be applicable any more. Through evaluation and review, emerging risks will be identified before they become too costly. This step is essential to the risk management program.

2.12.2.3 Protiviti

DeLoach (2000), Managing Director of Protiviti recognises five steps to implement ERM:

Step 1 is to conduct an enterprise risk assessment (ERA) to understand, assess and prioritise the critical risks. An ERA identifies and prioritises the

organisation's risks and provides quality inputs for purposes of formulating effective risk response.

Step 2 involves the articulation of the risk management vision and support thereof with a compelling value proposition. This step provides the economic justification to going forward. The risk management vision is a shared view of the role of risk management in the organisation and the capabilities desired to manage its key risks. To be useful, this vision must be grounded in specific capabilities (including policies, processes, competencies, reporting, methodologies and technologies required to execute the organisations response to managing its priority risks) that must be developed to improve risk management performance and achieve management's selected goals and objectives.

Step 3 entails the advancement of the risk management capability of the organisation for one or two priority risks. This step focuses the organisation on improving its risk management capability in an area where management knows improvements are needed.

Step 4 is the evaluation of the existing ERM infrastructure capability and development of the strategy for advancing it. It takes discipline to advance the capabilities around managing the critical risks. The policies, processes, organisation and reporting that instils that discipline is called "ERM infrastructure". The purpose of ERM is to eliminate significant gaps between the current state and the desired state of the organisation's capabilities around managing its key risks. Some examples include a common risk language, knowledge sharing to identify best practices, common training, a CRO, definition of risk appetite and risk tolerances, integration of risk response with business plans and supporting technology.

Step 5 entails the advancement of the risk management capabilities for key risks.

2.12.2.4 Accountancy Ireland publication

According to Dr Orna Duggan (2006:27), the risk management process should link seamlessly with the strategic planning and performance management cycles carried out in the organisation and should support the continued improvement and refinement of these processes. She proposes a five step approach which entails the following:

Step 1 is the identification of key risks undertaken in consultation with key personnel and in the context of corporate objectives.

Step 2 involves the ranking and prioritisation of risks on the basis of likelihood and impact.

Step 3 is the consideration of current and possible future risk management controls and the preparing of the risk register.

Step 4 entails the planning for ongoing risk management including the development of the Risk Management policy, allocation of risk ownership, reporting, review and update of the risk register.

Step 5 is embedding which involves the preparation and delivery of risk training material and should be carried out as early as possible after the first risk register has been prepared and at suitable intervals thereafter.

2.12.2.5 Compliance Week publication

In an article in the Compliance Week issue of 29 August 2007, Jaeger (2007) distinguished between the following five simple steps in the ERM process:

Step 1 starts at the top. An ERM program cannot succeed without the constant support of senior-level executives. They set the tone from the top for the whole organisation.

Step 2 involves building a team: Once the support from the top is in place, the focus should be on building a dedicated risk management committee that pervades all aspects of the organisation. This involves appointing a midlevel or senior level person from each division, expected to participate in risk management discussion.

Step 3 is risk identification. All possible risks that the organisation may face must be identified. Risks vary greatly, depending upon the organisation and the industry.

Step 4 entails the managing of risks. After all risks have been identified, an assessment of how to manage those risks should be made. This entails going through a total risk profiling which involves a disciplined methodology with a senior and very diverse group of executives to assess what risks the organisation are facing. Then, in subsequent meetings with specific individuals with the necessary knowledge and experience they would drill down to what the real risk exposures would be.

Step 5 involves the monitoring of risks. An ERM program is not something the board can implement in a quarter or one fiscal year and then left to mature at its own pace. An ERM program is a dynamic process that boards must internalise, regularly revising their ERM assumptions and the program's performance. Having a monitoring system in place tends to keep people diligent on mitigation action and realistic about risk assessments.

2.12.3 The derived enterprise-wide risk management process

From the abovementioned literature, it can be derived that a similar ERM process is followed by most of the organisations despite the fact that certain organisations divide the process in more steps than others. Based on the views of the authors, the following ERM process has been derived and is supported by further literature below:

2.12.3.1 Step 1 - Assign responsibilities

According to the position paper from the Institute of Internal Auditors (IIA) (2002), boards of directors, senior management, internal auditors, and external auditors are the cornerstones of the foundation on which effective corporate governance must be built. The primary risk management roles and responsibilities are set out in Table 2.2 below. The risk owners are also included as part of the risk management responsible people.

TABLE 2.2: WHO SHOULD BE RESPONSIBLE FOR WHAT?

	RISK MANAGEMENT RESPONSIBILITIES?	**PRIMARY ROLES IN CORPORATE GOVERNANCE**
Board of Directors	No	Provides risk management direction, authority, and oversight to senior management.
Senior Management	Yes	Has primary responsibility for ERM. Delegates risk management authority, and specify risk tolerance thresholds to risk owners. Reports ERM plans and performance results to the board of directors.
Risk Owners	Yes	Assign specific risk management authority and risk tolerance thresholds to other personnel. Report ERM plans and performance results to senior management.
Internal and External Auditors	No	Provide independent, objective assurance to senior management and the board of directors about the effectiveness of risk management, control, and governance processes.

(Source: Sobel & Reding (2004))

2.12.3.1.1 *The role of the Board of Directors*

The Board of Directors has a very important role to play in the ERM journey. The Board's duties entails that the Board is demonstrably and proactively involved in setting clear strategic objectives for the organisation, understands the risks threatening the realisation of those objectives and has put in place a policy and process for the management and oversight of those risks across the organisation. Executive management is also routinely and actively involved in the application of risk management policy and the operation of process. It is the responsibility of the Board of Directors to ensure that the risk management policy is understood throughout the organisation and the associated process is accepted as by all management as a "performance enhancing" activity for the business (Bramwell, 2006:14).

Corporate board members are devoting more time to enterprise risk management these days and taking a more aggressive approach to make headway on the sometimes-elusive goal, according to a new survey. The poll of 802 board members (and 235 general counsels asked about the same subjects) indicated that 45 percent of general counsels devoted more time to ERM in 2006 than in previous years. Topping the list of risks to manage were corporate governance changes and mergers and acquisitions (Aquilar, 2007).

The King II Report (2002:75) emphasises that the board of directors is responsible for the implementation of an effective and sustainable process of risk evaluation and the measurement of potential impact that the evaluation has on the organisation. Furthermore, the board of directors are responsible to address risks in a timely manner. This has a direct impact on the internal auditor which must give assurance to the board of directors on the adequacy and effectiveness of internal controls implemented to mitigate identified risks and exposure to the organisation.

According to the Ferma Risk Management standard (2003:12), the Board should, in evaluating its system of internal control, consider the nature and extent of downside risks acceptable for the company to bear within its particular business and the likelihood of such risks becoming a reality. They should also consider how unacceptable risks should be managed, and the company's ability to minimise the probability and impact on the business. The costs and benefits of the risk and control activity undertaken, the effectiveness of the risk management process, and the risk implications of board decisions are also important factors to be considered in the evaluation of the system of internal control.

2.12.3.1.2 *Champions of enterprise-wide risk management*

Traditionally, risk management has been a specialist subject, handled by staff with expertise in the area. The risk management process has tended not to be integrated into either the strategic or operational decision-making procedures of the organisation. However, it is becoming increasingly important for organisations to include all areas of the enterprise in the risk management process. The regulatory pressures now imposed on organisations, with increased focus on all aspects of corporate governance, require that risk management can no longer be left to be handled by experts in isolation. Senior executives, managers, and staff not only need to be aware of the issues, but also take an active role in the process (MarketWatch, 2006).

It is imperative that all personnel within an organisation should exercise risk management as part of their day-to-day activities. The importance of effective risk management in the organisation, as a whole is emphasised in the King II Report (2002:74).

Risk management is often being perceived to be the responsibility of a select group of individuals within the organisation instead of the duty of all employees. This is specifically true when dealing with assurance functions such as internal audit, and fraud management (DeLoach, 2000:25).

According to Barton *et al.* (2002), enterprise-wide risk management will succeed only in organisations where senior management is ready to put its full faith and effort into the program. Senior managers cannot just delegate the task of implementing ERM; they must be the champions of the effort, and adopting enterprise-wide risk management is a major cultural change for a company. To succeed, it needs commitment from the highest levels of management.

2.12.3.1.3 *Chief Risk Officer's (CRO) duties*

The COSO's ERM framework and a number of other best practices approaches provide some international guidelines on what the role of the CRO entails.

A CRO is responsible to establish and communicate the organisation's ERM vision to the organisation, and to determine and implement an appropriate ERM infrastructure. This process assists management with integrating risk management with the strategic management process; to develop and communicate risk management policies and limits; to identify risk ownership gaps and overlaps requiring resolution to ensure appropriate ownership of the priority risks; they work with appropriate executives to establish the control environment; to assist the executive team with monitoring the organisation's critical risks and finally to assists in reporting of risks from all levels within the organisation; to facilitate enterprise wide risk assessments and monitor the capabilities around managing the priority risks across the organisation, and to implement appropriate risk reporting to the board, audit committee and senior management (Protiviti, 2006:30-31).

Further responsibilities of a CRO are to act as a business coach to management by assisting them in designing and implementing suitable risk management architecture and regularly reviewing such systems for adequacy and effectiveness; to monitor the company-wide risk profile and ensure that major risks are identified and reported upwards; to assist the board of

directors in fulfilling their corporate governance responsibilities; to assist in the execution of the approved risk management process; to facilitate challenges and drive the integrated approach, but they are not responsible for risk management; they may have authority for managing a selection of significant risk types. The CRO is a member of the risk management committee and reports either to the CEO or another member of the board; oversees the corporate risk management function and is the ultimate champion of the corporate risk management framework process; and should provide the executive management team with some form of an ERM maturity model. (De la Rosa, 2007:10-11).

2.12.3.1.4 *Chief Audit Executive (CAE) duties*

Based on the Deloitte Risk Intelligence Series Issue no 5 "The Risk Intelligent Chief Audit Executive' article, the CAE provides assurance to the board that the key risks to both value preservation and creation have been identified; different scenarios have been assessed and stress-tested; inherent versus residual risk has been reliably assessed; the residual risk appears to be within the appetite of the company for the type of risk; controls are both effective and efficient; and management's reports are reliable (Deloitte, 2007:7).

Linking to the above the Institute of Internal Auditors (IIA) (2004a:xxix) defines Internal auditing as an independent, objective assurance and consulting activity designed to add value and improve an organisation's operations. It helps an organisation accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.

The responsibility of internal audit with regard to risk management and the extent of work to be performed by them are also set out by the King II report (2002:89). According to the King II report the internal audit function is responsible to assist the board, directors and management through consultation and facilitation in identifying, evaluating and assessing significant organisational risks to objectives, and by providing independent assurance as

to the adequacy and effectiveness of related internal controls and the risk management process.

2.12.3.2 Step 2 - Determination of business objectives

The determination of objectives of the risk management program entails deciding precisely what it is that the organisation expects its risk management program to do. One primary objective of the risk management effort is to preserve the operating effectiveness of the organisation (Meier, 2000:4).

It is of great importance that the ERM champions undertaking implementation of ERM obtains a comprehensive understanding of the organisation. They need to focus on the organisation's overall strategy, vision, mission, objective setting, risk appetite, risk tolerances, and the interrelationships therein before engaging in the ERM process. Clear goals and objectives are vital to success.

Schanfiled and Miller (2005) are of the opinion that it is critical that the risk management team clearly understand what the organisation does, how it buys, from whom it buys, how it sells and where it manufactures. Objective setting and company background in conjunction with an understanding of the internal environment - tone at the top, board of directors, integrity and ethical values, human resource policies and procedures - provides perspective on the business in order for the risk identification process to begin.

2.12.3.2.1 *Risk infrastructure*

ERM infrastructure facilitates three very important things with respect to ERM implementation. First, it establishes fact-based understanding about the organisation's risks and risk management capabilities. Second, it ensures there is ownership over the critical risks. Finally, it drives closure of gaps. ERM infrastructures (including an overall risk framework,

common language, policy and processes for assessing and managing risk) vary in form but are essential to driving throughout the organisation the idea that decision makers should consider risks (DeLoach, 2005).

2.12.3.2.2 *Risk frameworks*

Risk frameworks are a key component of any ERM programme. They provide personnel with a tool to assist in identifying sources of uncertainty. It is imperative that the risk framework be general in nature so that all sources and classifications of risk are included (DeLoach, 2000:52).

2.12.3.2.3 *Common business risk language*

The absence of a consistent language leads to miscommunication and oversights. Within an ERM programme a common language affords the following significant benefits according to the administrator (De La Rosa, 2003:151): It provides employees and other affected stakeholders with the ability to not only perceive risk as negative but also as possible areas of opportunity not previously considered. It also allows the organisation to aggregate risk exposures across multiple processes and business functions. Additionally it provides the board with the assurance that the shared risk management vision can be attained, as all stakeholders perceive key risk management terms in the same light. Lastly it allows for the effective identification and assessment of exposures while ensuring that potential sources of uncertainty are capitalised upon (DeLoach, 2000:59).

2.12.3.2.4 *Risk management policy*

When an organisation is listed on the New York Stock Exchange (NYSE) it is required to have a risk policy. According to the Deloitte presentation "The Risk Intelligent Enterprise - ERM done right" (Deloitte, 2006:8), the NYSE requires that the audit committee discusses with management the major financial risk exposures and the steps taken to monitor and control such

exposures; also that the audit committee should be satisfied with the company's risk assessment and risk management processes.

An organisation's risk management policy should set out its approach to and appetite for risk and its approach to ERM. The policy should also set out responsibilities for risk management throughout the organisation. It should also refer to any legal requirements for policy statements, e.g. for Health and Safety (Ferma, 2003:12).

Risk appetite refers to how much risk the organisation is willing to take. According to IRMSA Code of Practice the risk-taking traits of managers and directors can be classified according to risk-avers, risk-neutral and risk-taker styles (IRMSA: 45).

2.12.3.3 Step 3 - Identification and evaluation of risks

2.12.3.3.1 *Identification of risks*

Ferma (2003:6) states that risk identification sets out to identify an organisation's exposure to uncertainty. This requires an intimate knowledge of the organisation, the market in which it operates, the legal, social, political and cultural environment in which it exists, as well as the development of a sound understanding of its strategic and operational objectives, including factors critical to its success and the threats and opportunities related to the achievement of their objectives.

According to Bookstaber (1999:18), head of risk management of Moore Capital Management, risks can only be managed when they are identified and their possible outcomes are considered. Market risk can be managed because it is known that companies can default; operational risks because it is known that missteps are possible in settlement and clearing. Despite all the controllable risks, the greatest risks remain beyond our control. These are the risks we do not see, things beyond the veil. The challenge in risk management is how to deal with these unidentified risks. The answer is that

we cannot identify these risks directly but we can identify characteristics of risk management that will increase our ability to react to the risks.

Added to the above, the Ferma Risk management standard (2003:6) notes that risk identification should be approached in a methodical way to ensure that all significant activities within the organisation have been identified and all the risks flowing from these activities defined. All associated volatility related to these activities should be identified and categorised.

DeLoach (2005) indicates that the first step in implementing ERM is to conduct an enterprise risk assessment (ERA) to assess and prioritise the critical risks and formulates effective risk responses. According to him, an ERA enables you to understand your risks.

In the article from Deloitte 'Disarming the Value Killers: A Risk Management Study (Deloitte, 2005:1) it was noted that some of the greatest value losses were caused by exceptional events such as the Asian financial crisis, the bursting of the technology bubble, and the September 11th terrorist attacks. Yet many organisations apparently fail to plan for these rare but high-impact risks. Organisations should employ "stress testing", to ensure that their internal controls and business continuity plans can withstand the shock of a high impact event. Organisations should proactively plan and acquire the strategic flexibility to respond to specific scenarios.

There are various approaches and methods that can be used to identify risks. These may include scenario analysis to identify critical and significant business risks and entails that the business looks at the total picture. For example: a fire to a critical part of the business will not just damage equipment and buildings but will also result in business interruption. Another approach that is used is self-assessments done by various managers at different levels and different business units, as they are responsible to assess their own risk regularly due to constant changing. Additional approaches includes brainstorming; questionnaires; business studies which look at each business process and describe both the internal processes and external

factors which can influence these processes; industry benchmarking; risk assessment workshops; incident investigation; auditing and inspection; and hazard and operability studies (Ferma, 2003:15).

Examples of risk analysis methods and techniques include market surveys, prospecting test marketing; research and development and business impact analysis (Ferma, 2003:15).

Executive management should ensure that the ERM initiative is focused on the top 20 to 40 risks during ERM's initial development phases. This means allowing the ERM discipline to grow with the organisation's key processes whilst nurturing the ERM process with the right resources and right time (De la Rosa, 2006:11)

2.12.3.3.2 *Evaluation of risks*

Risk evaluation is used to make decisions about the significance of risks to the organisation and whether each specific risk should be accepted or treated (Ferma, 2003:10).

Evaluation means measuring the potential size of loss and the probability that it is likely to occur. The evaluation requires ranking of priorities as high impact, medium impact and low impact risks (Meier, 2000:4).

2.12.3.3.3 *Risk analysis and ranking*

All identified risks should be assessed in terms of impact and likelihood so that they can be prioritized and communicated. Risk estimation can be quantitative, semi-quantitative or qualitative in terms of the probability of occurrence and the possible consequence (Ferma, 2003:7). There are several qualitative and quantitative techniques to assess significance. Scales could be created to assess the probability of occurrence, either assuming no controls are in place (inherent risk) or considering controls known to be in place (residual risk).

Barton *et al.* (2002) noted that risks should be ranked on some scale that captures their importance, impact, severity, or dollar amount. This process assists management firstly in establishing the perceived importance of the risk and secondly by sorting risks according to their importance, management can use the list to develop a risk management strategy and to allocate resources efficiently.

Risk is analysed by combining estimates of consequences (impact) and probability (likelihood). According to the Vodacom Enterprise Risk Methodology (Meiring, 2006:5), this can be done by determining existing controls by identifying the existing management, systems and procedures that are currently controlling the risk, and by determining consequence and probability for each risk.

Consequence is defined as the positive or negative outcomes of decisions, events or processes. Risk events create consequences. Probability is defined as a measure (expressed as a percentage or ratio) of estimation of the change of occurrence (Meiring, 2006:5).

After completion of the risk analysis process, it is necessary to compare the estimated risks against risk criteria which the organisation has established. The risk criteria may include associated costs and benefits, legal requirements and concerns of stakeholders (Ferma, 2003:10).

2.12.3.3.4 *Risk integration*

Integration of risk and adopting an ERM approach is done in three steps as described in Table 2.3. Quantification of enterprise-wide risks gives you a better understanding of the consequence, frequency and likelihood of those risks.

TABLE 2.3: - THREE STEPS TO RISK INTEGRATION

Step Action	Methods
1. Identify all significant risks.	▪ List risks, assess risk, map risk
2. Measure risk and integrate best practices and tools	▪ Value at risk (VAR) and stress testing; earnings at risk (EAR) ▪ Apply financial tools to non-financial risks
3. Look enterprise-wide	▪ Look for: - Inconsistencies - Natural offsets - Transfer/financial opportunity

(Source: Barton *et al.* (2002))

2.12.3.3.5 *Risk profile*

The results of the risk analysis can be used to produce a risk profile, which gives a significance rating to each risk, and provides a tool for prioritising risk treatment/response efforts. This ranks each identified risk so as to give a view of the relative importance. This process allows the risk to be mapped to the business area affected, describes the primary control procedures in place and indicates areas where the level of risk control investment might be increased, decreased or reapportioned (Ferma, 2003:9).

2.12.3.4 Step 4 - Determination of appropriate risk treatment/response strategies

Avoid, share, reduce, accept, and exploit are the various options available for management to consider in implementing risk responses (also known as risk mitigation strategies). There are qualitative and quantitative (cost versus benefit) considerations. It also may be necessary to use experts to expedite the process and ensure all issues are reviewed (e.g., actuaries or environmental experts) (Schanfield & Muller, 2005).

Ferma (2003:10) defines risk treatment or response as the process of selecting and implementing measures to modify the risk. Risk treatment/response includes as its major element, risk control/mitigation, but extends further to, for example, risk avoidance, risk transfer and risk financing.

Risk treatment devices are used in deciding which technique to use to deal with a given risk. The risk's size, potential loss, its probability and the resources that would be available to meet the loss if it should occur is considered (Meier, 2000:4).

Companies are choosing various combinations of acceptance, transfer, and mitigation to manage risk. Some risks are inevitably difficult to control and organisations are forced to accept them. However, these risks should be regularly monitored. Risks can also be transferred, for example insurance. In order to mitigate risks effective controls should be put in place. Decisions regarding control (an application of mitigation), acceptance, and transfer are dynamic – they must be continuously re-evaluated. There are choices to be made as to how risks will be addressed, and those choices have consequences (cost versus benefits). Management needs to determine how these risks should be mitigated. Seek creative solutions and transfer risk where economic opportunities exist (Barton *et al.*, 2002).

The implementation of the decision is the decision to retain a risk. When an organisation decides to retain a risk they establish policies and procedures to reduce or eliminate the probability/frequency of occurrence and the severity of the impact (Meier, 2000:4).

2.12.3.5 Step 5 - Assign responsibility to each risk

All risks should be allocated to the relevant process owners. Accountability helps to ensure that ownership of the risk is recognised and the appropriate management resource allocated (Ferma, 2003:9).

2.12.3.6 Step 6 - Risk measurement

By measuring risk, an organisation does not waste resources, allocate capital inefficiently, or spend time on the least risky areas. However, this is not an easy task. The most measurable risks are normally the high frequency but low impact risks (Barton *et al.*, 2002).

Financial risk should be measured with the most sophisticated and relevant tools available, such as value at risk (VAR) and stress testing. The most developed areas for risk measurement are in financial risks. The most common approaches for measuring and assessing financial risk are VAR and stress testing. VAR and stress testing can be used to measure financial risk and market risk. VAR is a monitoring tool and not a forecasting tool. Other tools include earnings at risk (EAR) which measures the effect of risk on earnings based on the organisations risk appetite and potential appetite of investors (Barton *et al.*, 2002).

Based on the above it is essential to develop sophisticated tools and measures that meet the organisation's needs and that management can easily understand. More determination should be applied to measuring non-financial risks wherever possible. By ranking and then measuring (if possible) risk, management becomes aware of the real risks that they need to effectively manage. Only on this basis can value-maximizing decisions be made. Risk measurement (specifically for non-financial risks) is one area where innovation and further research is required (Barton *et al.*, 2002).

2.12.3.7 Step 7 - Evaluation and review

Within the risk management process the business environment changes; new risks arise and old ones disappear. Techniques that were appropriate last year may not be relevant this year and so constant attention to risk is required. Through evaluation and review, the decisions are reviewed and mistakes can be discovered before it becomes too costly (Meier, 2000:4).

The monitoring process should provide assurance that there are appropriate controls in place for the organisation's activities and that the procedures are understood and followed. Changes in the organisation and the environment in which it operates must be identified and appropriate change made to systems (Ferma, 2003:14).

The King II code (2002:75) notes that the monitoring of risks should be linked to key performance indicators and organisational objectives so that the accuracy of the risk assessment and the effectiveness of internal controls can be evaluated objectively. The use of Key Risk Indicators (KRI) enables ongoing monitoring of risks for movements in impact and likelihood. These movements can be caused either by changes in the inherent nature of the risk or by changes in the design and performance of control activities in place to mitigate risk. By carrying out monitoring through key risk indicators, organisations can ensure that any dynamic changes in their risk profile are noted as they happen and that necessary action is taken in a timely manner. For key risk indicators to work effectively there must be well-defined risk and control ownership and accountability. Risk and control owners have a key role to play in enabling this method of ongoing monitoring of risk to be embedded throughout the organisation.

Lessons learnt in practice with regard to Key Risk Indicators (KRI) (KPMG, 2006:5 - 12):

- There is a natural resistance by management to use KRI. Management views key risk indicators as a measure of how well they are doing their job. KRI make the ERM philosophy come to life.
- KRI demonstrate the value of risk management.
- KRI have different connotations at different levels within the company. KRI are sometimes equitable to KPI and accordingly KPI can also be indicators of risk.
- Most companies have numerous indicators, which are tracked. Instead of starting a process that is relatively new, Change Management principles could be applied. A review should be performed to determine which risks have not already been assigned KRI.
- Management is often reluctant to adopt KRI and the tendency exists to amend risks previously identified. KRI serve to reveal misperceptions regarding risks. The KRI could reveal misperceptions regarding risks. The KRI could reveal that a risk is not as high as previously assessed. Data trends need to be monitored to re-craft the risk focus, whereby perception is converted into factual data analysis.
- Ownership of KRI need to be defined and must be very clear, as the tendency exists to circumvent ownership by stating that the risk is not manageable within a certain functional area in the company. Management should take ownership of the KRI for their individual functional areas. Ownership of KRI resides with management.
- The responsibility for gathering data for KRI needs to be addressed. Management accounts can be used to match information to the risk register and determine whether there are any gaps. The risk owner can be responsible for tracking the information on a scheduled basis.
- Deriving KRI is often perceived to be a tedious and burdensome process. Management is not necessarily schooled in respect of KRI so the CRO should assist in this regard.
- KRI should be accurately aligned to the risk register. They should also track emerging risks, because risks may materialise in new areas.

- Regular risk reviews should occur. KRI could prove that risks need to be re-assessed.
- KRI should not be viewed in isolation, but in combination with other indicators. Information needs to be linked by looking for correlation between risks. A single KRI could give an indication of many other risks, which need to be tracked.
- KRI could also reveal potential opportunities for a business.
- Data analysis is critically important. The analysis of the data results in ERM moving into operational areas.
- The CRO should not manage KRI. It should be performed by functional managers/risk owners. The CRO may need to assist management with deriving KRI and has a supervisory role for KRI.
- Management is required to respond at strategic, tactical and operational level from an ERM perspective so the chosen KRI should reflect this.
- KRI should lead to risk-related decisions in normal management meetings, regardless of who has devised the KRI.

2.12.3.8 Step 8 - Risk reporting and communication

2.12.3.8.1 *Internal reporting*

A number of organisations lacked access to current information required for senior management to respond quickly to emerging problems. Organisations need to improve their internal information systems, and communication mechanisms to ensure that senior management and boards of directors receive accurate, near real-time information on the causes, financial impact, and possible solutions of control procedures (Deloitte, 2005:1).

Different levels within an organisation require different information from the ERM process as discussed below (Ferma 2003:11 –12):

The Board of Directors should know about the most significant risks facing the organisation. They should know the possible effects on shareholder value of

deviations to expected performance ranges, ensure appropriate levels of awareness throughout the organisation, know how the organisation will manage a crisis, know the importance of stakeholder confidence in the organisation, know how to manage communications with the investment community, be assured that the ERM process is working effectively, and publish a clear ERM policy covering risk management philosophy and responsibilities.

Business units should be aware of risks, which fall into their area of responsibilities, and the possible impacts these may have on other areas and the consequences other areas may have on them. They should have performance indicators, which allow them to monitor the key business and financial activities, progress towards objectives and identify developments that require intervention. They should also have systems that communicate variances in budgets and forecasts at appropriate frequency to allow action to be taken, and report systematically and promptly to senior management any perceived new risks or failures of existing control measures.

Individuals should understand their accountability for individual risks, understand how they can enable continuous improvement of risk management response, understand that ERM and risk awareness are key parts of the organisation's culture, and report systematically and promptly to senior management any perceived new risks or failures of existing control measures.

2.12.3.8.2 *External reporting*

Good corporate governance requires that companies adopt a methodical ERM approach which protects the interest of their stakeholders, ensures that the Board of Directors discharges its duties to direct strategy, guild value and monitor performance of the organisation, and ensures that management controls are in place and performing adequately. A company needs to report to its stakeholders on a regular basis setting out its risk management policies and the effectiveness in achieving its objectives. Increasingly stakeholders

look to organisations to provide evidence of effective management of the organisation's non-financial performance in such areas as community affairs, human rights, employment practises health and safety, and the environment. Formal reports should address the control methods, the processes used to identify risks and how they are addressed by the ERM systems, the primary control systems in place to address significant risks and the monitoring and review systems in place. In addition, any significant deficiencies uncovered by the internal control system, should be reported together with the steps taken to deal with them (Ferma, 2003:11-12).

2.12.3.9 Step 9 - Embedding the process of enterprise-wide risk management

The final step is embedding of the process of ERM. This involves the preparation and delivery of risk training material and should be carried out as early as possible after the first risk register has been prepared and at suitable intervals thereafter. This process is frequently carried out at corporate level (producing an enterprise risk register) and at divisional level, producing a cascade effect in the management of risks (Duggan, 2006).

Various ways can be used to create risk awareness and includes face-to-face communication, risk assessment, analytical tools, intranet, risk philosophy, SVA, and EAR. Companies that embrace enterprise-wide risk management face the daunting task of instilling risk awareness in a corporate culture focused on other objectives (Barton *et al.*, 2002).

CHAPTER 3
THE DERIVED ENTERPRISE-WIDE RISK MANAGEMENT PROCESS

3.1 INTRODUCTION

From the literature review in Chapter 2 an enterprise-wide risk management process emanated. Key learnings have been compiled from successful ERM implementations that could potentially be useful to other organisations in developing and expanding on existing ERM practices to facilitate the preparation and practical implementation of ERM in order to give assurance to all stakeholders that all potentially significant risks are identified and managed. The key learnings are discussed using the steps formulated in the devised ERM process.

3.2 THE DERIVED ENTERPRISE-WIDE RISK MANAGEMENT PROCESS

From the literature review it is evident that many times organisations embark on an ERM initiative and have not defined where they are and what they want to achieve. It is essential that the risk management objectives be defined before embarking on the ERM process (Meier, 2000:4).

As per Chapter 2, every organisation is unique and the ERM process must be tailored to specific needs and circumstances. No one-size-fits-all ERM solution exists.

The following nine-step ERM process has been devised from all the proposed processes discussed in Chapter 2:

Step 1 entails the assignment of responsibilities. Commitment from the Board of Directors is obtained and roles and responsibilities for the ERM initiative are established.

In Step 2 the business objectives are determined. Understanding the business model, and articulating and communicating the business objectives of the organisation are essential. The risk appetite of the organisation is determined which indicates how much risk the organisation is prepared to take on. The appropriate internal environment is established, including a risk management policy and process for assessing and managing risk.

Step 3 is the identification and evaluation of risks. Key risks and vulnerabilities are identified that are potential threats to the achievement of business objectives. The significance of risks is assessed and the impact and likelihood of the threat is evaluated.

Step 4 involves the determination of appropriate risk treatment/response strategies. Risk treatment is the process of selecting and implementing measures and control to modify and mitigate the risk. Risk treatments include avoidance, transfer, diversifying, implementing of additional controls, or shared risk.

Step 5 consists of the assignment and management of specific risks. A decision is made on who has the responsibility and authority to take risk on behalf of the company. Control activities and other response activities are implemented.

Step 6 entails the measuring of risks. This step involves the quantification of risks. Certain risks are however very difficult, if not impossible to measure.

Step 7 is the evaluation and review of risks. This step involves the constant evaluation of risks to ensure that the impact of changes on the environment is assessed and necessary actions to mitigate additional risks are taken on a timely basis.

Step 8 entails the monitoring and coordinating of the risk management processes and the outcomes. Communication of information on risks in a

consistent manner at all levels in the organisation is essential to the ERM process.

The final step is embedding the process of ERM. This step involves the determination of the capability to manage risk on an integrated and sustainable basis. Risk awareness is created throughout the organisation.

3.3 KEY LEARNINGS

It is evident from research that the ERM process is a lengthy process. There are certain steps to be followed to ensure an effective ERM process. Key learnings for the journey towards an effective ERM process were documented as a result of commonalities identified in the various case studies researched, journals and articles by a number of authors. These key learnings were documented following the derived ERM process above.

3.3.1 Assign responsibilities

3.3.1.1 The role of the Board of Directors

Key learning 1: The board has overall responsibility for ensuring risks are properly managed within the organisation.

Key learning 2: Downside (risks) risk culture needs to be challenged to capture upside (opportunities) potential within outputs of the ERM process.

3.3.1.2 Champions of enterprise-wide risk management

Key learning 3: While ultimate responsibility for ERM starts at the top, everyone who matters within an organisation should participate to some extent in the ERM process. While several executives have significant responsibilities for ERM, including CRO, CFO, CLO, CEO and CAE, the ERM process works best when all key managers of the organisation contribute and

support the ERM process. This could only happen if performance goals are clearly articulated and the appropriate individuals are held accountable for results.

Key learning 4: The predominant practice for integrating risk management is to build an organisational philosophy and culture in which everybody is a risk manager. Senior management needs to create a culture emphasising the central importance of ethical behaviour, quality control, and risk management.

Key learning 5: Everyone in the organisation plays a role in ensuring successful ERM but the primary responsibility for identifying risks and managing risk lies with management. Therefore a prerequisite for implementation of ERM is the commitment of one or more champions at the senior management level. It is important that all managers, employees and stakeholders see the champion's involvement.

Key learning 6: Identify 'right' stakeholders and continue to engage with them throughout the process. Recognise business as part of the ERM project to encourage ownership of approach and results.

Key learning 7: Informal and formal teams are a mechanism that organisations use to manage risks. Teaming brings together various risk attitudes and brings fresh thinking to issues and solutions.

3.3.1.3 Risk Officer's (CRO) duties

Key learning 8: It is important to set up a responsibility centre for risk management that is headed by possibly the CRO.

3.3.1.4 Chief Audit Executive (CAE) duties

Key learning 9: The internal audit function plays a key role in implementing risk management throughout an organisation. Examples of their assistance are facilitating self-assessment workshops; monitoring and reporting on

management significant risks; providing advice, raising awareness of risk management; reviewing processes of managing risks, and sitting on the risk management committee.

3.3.2 Determining business objectives

Key learning 10: A clear understanding of the business is of vital importance before embarking on an ERM process. Management is responsible to align the ERM goals and objectives with overall business objectives, strategies and performance goals and communicates these throughout the organisation through written policies and procedures. ERM responsibilities, authorities and accountabilities should be assigned to appropriate personnel so that everyone understands their roles.

3.3.2.1 Risk infrastructure

Key learning 11: Risk management infrastructures (including an overall risk framework, common language, policy and processes for assessing and managing risk) vary in form but are essential to driving throughout the organisation the idea that decision makers should consider risks.

3.3.2.2 Risk frameworks

Key learning 12: It is imperative that the risk framework be general in nature so that all sources and classifications of risk are

3.3.2.3 Common business risk language

Key learning 13: Use a simple, common business risk language. A common business risk language enables managers to talk with individuals from the boardroom to the boiler room in terms that everybody understands.

Key learning 14: Open communication is necessary for risk management to succeed.

Key learning 15: Clear definition of risk is essential to avoid risk overlap and overestimation of exposure.

3.3.2.4 Risk management policy

Key learning 16: Know your company and shareholders' appetite for risk.

3.3.3 Identification and evaluation of risks

3.3.3.1 Identification of risks

Key learning 17: To manage effectively in today's business environment, organisations are required to make a formal, dedicated effort to identify all their significant risks by conducting an enterprise risk assessment (ERA) and prioritise critical risks.

Key learning 18: Various risk identification and risk analysis approaches, methods and techniques are available to identify risk. A critical success factor for successful risk identification is that the process of identification should be dynamic and continuous.

Key learning 19: Executive management should ensure that the ERM initiative is focused on the top 20 to 40 risks during ERM's initial development phases. This means allowing the ERM discipline to grow with the organisation's key processes whilst nurturing the ERM process with the right resources and right time.

3.3.3.2 Evaluation of risks

Key learning 20: Risk evaluation is used to make decisions about the significance of risks to the organisation and whether each specific risk should be accepted or treated.

3.3.3.3 Risk analysis and ranking

Key learning 21: Risks should be analysed in terms of impact and on some scale of frequency, likelihood or probability. Risk measurement can assist organisations in knowing the true importance of a risk and risk ranking can assist management in making risk-based decisions.

3.3.3.4 Risk integration

Key learning 22: Risk integration consists of three processes, which include the identification of significant risks, the measurement of risk, and integration with best practices.

3.3.3.5 Risk profile

Key learning 23: A risk profile can be used by organisations to have an enterprise-wide view of risk management and thereby enable them to identify and respond to the most important risks.

3.3.4 Determination of appropriate risk treatment/response strategies

Key learning 24: Avoid, share, reduce, accept, and exploit are the various options available for management to consider in implementing risk responses (also known as risk mitigation strategies). There are qualitative and quantitative (cost versus benefit) considerations. It also may be necessary to use experts to expedite the process and ensure all issues are reviewed.

3.3.5 Assign responsibility to each risk

Key learning 25: All risks should be allocated to the relevant process owners. Accountability helps to ensure that ownership of the risk is recognised and the appropriate management resource allocated.

3.3.6 Risk measurement

Key Learning 26: By measuring risk, an organisation does not waste resources, allocate capital inefficiently, or spend time on the least risky areas. However this is not an easy task. The most measurable risks are normally the high frequency but low impact risks.

Key learning 27: Sophisticated tools and measures should be developed that meet the organisation's needs and that management can easily understand.

Key learning 28: It is difficult to measure all risks. More determination should be applied to measuring non-financial risks wherever possible. By ranking and then measuring (if possible) risk, management becomes aware of the real risks that they need to effectively manage.

3.3.7 Evaluation and review

Key Learning 29: The monitoring process should provide assurance that there are appropriate controls in place for the organisation's activities and that the procedures are understood and followed. Changes in the organisation and the environment in which it operates must be timely identified and appropriate change made to systems.

Key learning 30: KRI have been successful in bringing a number of insights to the attention of executives. This often leads to a better response to risk from different levels in the organisation.

3.3.8 Risk reporting and communication

Key Learning 31: Risk reporting is done internally and externally to the organisation.

3.3.8.1 Internal reporting

Key Learning 32: A number of organisations lacked access to current information required for senior management to respond quickly to emerging problems. Organisations need to improve their internal information systems and communication mechanisms to ensure that senior management and boards of directors receive accurate, near real-time information on the causes, financial impact, and possible solutions of control procedures.

Key Learning 33: Different levels within an organisation require different information from the ERM process:

3.3.8.2 External reporting

Key learning 34: A company needs to report to its stakeholders on a regular basis, setting out its risk management policies and the effectiveness in achieving its objectives.

3.3.9 Embedding the process of enterprise-wide risk management

Key Learning 35: Various methods can be used to create risk awareness and do training which includes face-to-face communication, risk assessment, analytical tools, intranet, risk philosophy, SVA, and EAR amongst others. .

Key learning 36: Risk management training, as part of a corporate training curriculum, helps integrate risk. Topics may include: risk assessments, best practices, legislative requirements, safety, objectives for managing risk, and risk-awareness training to ensure that all managers consider risk.

Key Learning 37: Making risk consideration a part of the decision-making process is an essential element to enterprise-wide risk management.

3.3.10 Use of consultants

Key Learning 38: When consultants are used they should supplement, not replace, senior management involvement in the risk management effort.

Key Learning 39: Whilst risk identification can be carried out by outside consultants, an in-house approach with well communicated, consistent and co-ordinated processes and tools is likely to be more effective. In-house ownership of the risk management process is essential.

3.3.11 Enterprise-wide risk management software

Key Learning 40: A working and flexible ERM approach should be in place before implementing a software solution. "If you automate a mess you have an automated mess!"

CHAPTER 4
CONCLUSIONS AND RECOMMENDATIONS

4.1 CONCLUSIONS

From all the case studies and other relevant information researched it is evident that every organisation follows different steps and phases to get to their ERM solution. No 'one size fits all' solution exists. As stated by Barton, *et al.* (2002) "A cookbook recipe for implementing ERM is not feasible because so much depends on the culture of the company and the change agents who lead the effort." The implementation of any new ERM process will have some or other disruptive effect due to the change management aspects.

It is important to understand that the ERM process is a journey with no finite end. It is an interactive process and needs commitment from top management to succeed. All the organisations that have successfully implemented ERM had one common belief with regard to the implementation of ERM. They believed that ERM was creating, protecting and enhancing value by managing ERM.

An enterprise wide approach to business risk management will assist executives in meeting the challenges they face by improving the linkage of risk and opportunity during the strategy setting process and positioning risk management as a differentiating skill in managing the business. The importance of effective risk management in the organisation as a whole, are emphasised in this report.

4.2 RECOMMENDATIONS

The key lessons learnt from the study are summarised in the following Key Success factors (KSF) that are recommended for value adding ERM through effective implementation, embedding, monitoring and assurance over ERM:

1. Recognise and understand that ERM is a journey with an indefinite end. The process should be ongoing and momentum sustained.
2. An uncomplicated design for ERM is vital to instil an effective ERM system successfully.
3. ERM should be integrated into the culture of the organisation with an effective policy and a programme led by the most senior management.
4. The responsibility and support for risk management should be at the highest executive level. Clear delineation of roles and responsibilities is necessary. The CRO and the team will then become responsible for risk management throughout the organisation. This form of organisation ensures that risks will be viewed taking a comprehensive approach.
5. Every employee should be part of the ERM framework. Responsibility should be assigned throughout the organisation to each manager and employee responsible for management of risk as part of his or her job description. Guidelines and rules should be defined to describe how the company is to deal with risks in the future.
6. A clear understanding and knowledge of ERM should exist.
7. A risk language that everyone in the organisation understands should be developed.
8. All strategic and investment decisions should be based on the processes of risk management.
9. Risk management should be aligned with strategic and business objectives. ERM is a risk management trend worth exploring during the strategic planning process. Business managers who once thought that mitigating risk was their only goal are beginning to understand that good, holistic risk management can create competitive advantages and improve shareholder value.
10. Everyone in the organisation should think broadly about the expansive range of risks that are facing the organisation.
11. All information derived from the ERM system should be made available to decision makers on a timely basis.
12. No organisation can effectively manage risk and achieve its business objectives without accurate, timely, and comprehensive monitoring and

reporting. It supports accountability, performance measurement and reward and thus promoting operational efficiency at all levels.

Some of the most important challenges for implementing an effective and value adding ERM process include the following:

1. Lack of standardised risk terminology (language), valuation methods, reporting and coordination within organisations.
2. Lack of alignment between risk management and the existing planning process.
3. Lack of clearly defined roles, accountability and information flows.
4. Cultural opposition to change.
5. Lack of strong support from top management.
6. Lack of sufficient resources for ERM.
7. To maintain the stamina needed for ERM.
8. Cost of implementing ERM is very high.

The successful implementation of ERM is not an easy task but it is no longer a "nice to have". In today's challenging global economy, business opportunities and risks are constantly changing and therefore a dynamic and robust ERM process should be implemented to ensure effective management of risks. As proven, the mismanagement of risks can carry an enormous price.

4.3 RECOMMENDATION FOR FURTHER RESEARCH

Risk measurement (specifically for non-financial risks) is one area where innovation and further research is required. Many tools and techniques exists to quantify and measure financial risks, but some risks, for example litigation and other legal risks, operational risks such as administrative errors and fraud, natural disasters, HIV/Aids, skills shortages, fraudulent acts by executives and employees, fictitious transactions, insider trading, IT and data security and harassment in the workplace are not easily quantifiable and therefore the impact is unknown.

REFERENCES

AQUILAR, M.K. 2007. Report: ERM sinking into directors' heads. *Compliance Week,* 29 August.

ARMINAS, D. 2003. Managing risk set to be key task purchasers in 2003. *Supply Management*, 8(1): 9.

ARTHUR ANDERSEN. 1995. The economist intelligence unit. Managing business risk: An Integrated Approach.

BARTON, T.L., SHENKIR, W.G. & WALKER, P.L. 2002. Making enterprise risk management pay off: how leading companies implement risk management. *Financial Times,* Prentice Hall. February 08. 272 p.

BERNSTEIN, P.L. 1998. Against the gods. 2nd ed. Canada: Wiley.

BEST'S REVIEW. 2005. Risk Managers Want to Use Enterprise Risk Management, 106(6): 115. October.

BOOKSTABER, R. 1999. Risk management in complex organisations. *Financial Analyst Journal,* 55(2): 18-20. March/April.

BRAMWELL, P. 2006. A pragmatic approach to enterprise risk management. IRM Risk Forum. Keele University. 14. September.

COHEN, F.L. & PEACOCK, J.M. 1998. Managing risk to increase shareholder value: new concepts and tools. In pursuit of the upside: leading thinking on issues of risk management. A collection of PWC Risk Professionals. South Africa: The Institute of Internal Auditors.

COLVYN, G. 2006. Managing in chaos. *Fortune,* October 2.

COMMITTEE OF SPONSORING ORGANISATIONS OF THE TREADWAY COMMISSION. 2004a. Enterprise risk management – integrated framework: application techniques. [S.l]: COSO.

COMMITTEE OF SPONSORING ORGANISATIONS OF THE TREADWAY COMMISSION. 2004b. Enterprise risk management – integrated framework: executive summary framework. [S.l]: COSO.

COSO ***see*** Committee Of Sponsoring Organisations Of The Treadway Commission.

CRONJE, J.J.L., DE SWARDT, C.J., MALOBOLA, L., DE BEER, J.S., MUTEZO, A & BOTHA, E. 2004. Ondernemingsrisikobestuur. Departement Sakebestuur, Unisa.

DE LA ROSA, S. 2003. Common Language and Strategies. Chapter 8. University of Pretoria, 152.

DE LA ROSA, S. 2004. Integrating risk management and internal audit an internal audit perspective. *Internal Audit Advisor*, 20-25. December.

DE LA ROSA, S. 2006. ERM Touchstones. *Internal Audit Advisor*, 10-11. December.

DE LA ROSA, S. 2007. Taking a closer look at the role of Chief Risk Officer. *Internal Audit Advisor*, 10 - 11. March.

DELOACH, J. 2005. Enterprise risk management: practical implementation ideas. MIS Super Strategies Conference. April. [Web:] http://www.knowledgeleader.com/KnowledgeLeader/Content.nsf/Web+Content. [Date accessed: 16 Mar. 2007].

DELOACH, J. W. 2000. Enterprise-wide risk management: strategies for linking risk and opportunity. Great Britain: Pearson Education Limited.

DELOITTE. 2005. Disarming the value killers: a risk management study, 1-12.

DELOITTE. 2006. The risk intelligent enterprise: ERM done right, 1-8.

DELOITTE. 2007. The risk intelligent chief audit executive. *Risk Intelligence Series,* 5: 1-7.

DICKINSON, G. 2001. Enterprise risk management: its origins and conceptual foundation. Geneva Papers on Risk & Insurance – Issues & Practice, 26(3): 360-366. July.

DUGGAN, O. 2006. Enterprise risk management: the challenge for the public sector. *Accountancy Ireland,* 38(4): 25-27. August.

ECONOMIST INTELLIGENCE UNIT. 1995. In cooperation with Arthur Andersen & Co. Managing business risks - an integrated approach, New York: 2.

ESPERSEN, D. 2007. The language of risk. *Internal Auditor.* 69-73, June.

FEDERATION OF EUROPEAN RISK MANAGEMENT ASSOCIATES. 2003. Ferma. A risk management standard. 2-15.

FERMA **see** Federation of European Risk Management Associates.

GRAY, I. & MANSON, S. 2005. The audit process: principles, practice and cases. 3rd ed. London: Thomson. 891 p.

IFAC (Financial and Management Accounting Committee). 1999. Enhancing shareholder wealth by better managing business risk. Director General. International Federation of Accountants. New York, USA.

INSTITUTE OF DIRECTORS IN SOUTHERN AFRICA. 2002. *King Report on Corporate Governance for South Africa 2002.*: Institute of Directors in Southern Africa. Parkland, South Africa.

INSTITUTE OF INTERNAL AUDITORS. 2002. Recommendations for improving corporate governance.

INSTITUTE OF INTERNAL AUDITORS. 2004a. *The Professional Practices Framework. 2004.* The Institute of Internal Auditors Research Foundation. 2nd ed. Altamonte Springs, Florida.

INSTITUTE OF INTERNAL AUDITORS. 2004b. *The role of Internal Auditing in Enterprise-wide risk management. Position Statement.*

INSTITUTE OF RISK MANAGEMENT SOUTH AFRICA. 2002. [Web:] http://www.irmsa.org.za [Date accessed: 16 Feb 2007].

INSTITUTE OF RISK MANAGEMENT SOUTH AFRICA. Code of Practice. 97 pages.

JAEGER, J. 2007. Thinking globally, acting locally on ERM. *Compliance Week,* 29. August.

KEELE UNIVERSITY. 2006. Quantification and risk exposure, 9-10.

KING II REPORT ON CORPORATE GOVERNANCE FOR SOUTH AFRICA ***see*** Institute of Directors in South Africa.

KPMG. 2006. Enterprise risk management risk laboratory: key risk indicators, 2–14.

LALOUX, O. 2004. Greater drive for enterprise-wide risk management. *Finance Week,* 44-45, 17 May.

LAYTON, M. & FUNSTON, R. 2006. Deloitte - the risk intelligent enterprise: ERM done right, 2-8.

MARKETWATCH: GLOBAL ROUND UP. 2006. 5(11): 172. November.

MEIER, R.L. 2000. Integrating enterprise-wide risk management concepts into industrial technology curricula. *Journal of Industrial Technology,* 16(4): 1-6, August - October.

MEIRING, W. 2006. Vodacom Group (Pty) Ltd. Enterprise Risk Methodology, 1-15.

PROTIVITI. 2006. Independent risk consulting. *Guide to Enterprise Risk Management. Frequently asked Questions.* 144 p.

PROTIVITI. 2007. U.S. Risk barometer report [Web] http://www.protiviti.com/portal/site/pro-us/menuitem. [Date of access: 7 Sept. 2007].

PUSCHAVER, L. & ECCLES, R.G. 1998. In pursuit of the upside: the new opportunity in risk management. In pursuit of the upside: leading thinking on issues of risk management. A collection of PWC Risk Professionals. South Africa: The Institute of Internal Auditors.

SAMMER, J. 2001. Looking for risk in all the right places. [Web:] http://wwwbfmag.com/magazine/archives/article.html?articleD=13736. [Date of access: 22 Jun. 2007].

SAWYER, L.B., DITTENHOFER, M.A., & SCHEINER, J.H. 2003. *Sawyer's internal auditing: the practice of modern internal auditing.* 5th ed. Altamonte Springs, Florida: Institute of Internal Auditors.

SCHANFIELD, A. & MILLER, M. 2005. A sustainable approach to ERM: as best practices begin to emerge, one company uses a phased plan to create a fully functioning, integrated enterprise. *Internal Auditor.* April. [Web:]

http://www.findarticles.com/p/articles/mi_m4153/is_2_62/ai_n13821970. [Date of access: 16 Feb. 2007].

SESEL, J. 2000. The history of professional risk management. [Web:] http://www.siliconrose.com.au/Articles.htm. [Date of access: 21 May 2007].

SHOUGH, R. 2006. Deloitte. *The Evolving Nature of Risk Management.* 10th Southern African Internal Audit Conference., 1 - 29. August.

SOBEL, P & REDING, K.F. 2004. Aligning corporate governance with enterprise risk management. *Management Accounting Quarterly.* 5(2): 31. Winter.

STEWART, T.A. 2002. Managing risk in the 21st Century. *Fortune.* 7 February, 202.

SYCIP GORRES VELAYO & CO. Bulletin. 2004. Enterprise risk management in the new era of governance. [Web:] http://www/sgv.com.ph. [Date of access: 22 Jun. 2007].

ULICK, J. 2002. Worldcom's financial bomb. [Web:] http://www.money.cnn.com/2002/06/25 news/worldcom/. [Date of access: 16 Mar. 2007].

UNIVERSITY OF SURREY. 2005. Risk management history. [Web:] http://portal.surrey.ac.uk/portal/page?_pageid=823,181080&_dad=portal&schema=PORTAL . [Date of access: 1 Mar. 2007].

VALSAMAKIS, A.C., VIVIAN, R.W. & DU TOIT, G.S. 2003. Risk management. 2nd ed. Sandton: Heinemann Higher.

VALSAMAKIS, A.C., VIVIAN, R.W. & DU TOIT, G.S. 2005. Risk management: managing enterprise risks. 3rd ed. Sandton: Heinemann Higher.

WARING, A. & GLENDON, A.I. 2001. Managing risk: critical issues for survival and success into the 21st century. London: Thomson.