EPIRISMM: AN ENTERPRISE INFORMATION RISK MANAGEMENT MODEL

by

NEIL LATEGAN

Dissertation

submitted in fulfilment

of the requirements

for the degree

Magister Technologiae

in

Information Technology

in the

Faculty of Engineering, the Built Environment and

Information Technology

of the

Nelson Mandela Metropolitan University

Supervisor: Professor Rossouw von Solms

December 2006

Declaration

I, Neil Lategan, hereby declare that:

The work in this dissertation is my own work.

All sources used or referred to have been documented and recognised.

This dissertation has not previously been submitted in full or partial fulfilment of the requirements for an equivalent or higher qualification at any other recognised educational institution.

_____

Neil Lategan

With acknowledgement for valued assistance towards the finalisation of my dissertation:

To God, for creativity, strength, motivation and everything else.

****

To Prof Rossouw von Solms for guidance, encouragement and the sharing of a wealth of experience.

****

To the National Research Foundation and the NMMU for financial support in the pursuance of my goals.

In light of knowledge attained, the happy achievement seems almost a matter of course, and any intelligent student can grasp it without too much trouble. But the years of anxious searching in the dark, with their intense longing, their alterations of confidence and exhaustion and the final emergence into the light – only those who have experienced it can understand it.

Albert Einstein

ABSTRACT

Today, information is considered a commodity and no enterprise can operate without it. Indeed, the information and the supporting technology are pivotal in all enterprises. However, a major problem being experienced in the business environment is that enterprise risk cannot be managed effectively because business and information-related risk are not congruently aligned with risk management terminology and practices. The business environment and information technology are bound together by information. For this reason, it is imperative that risk management is synergised in the business, ICT (Information and Communication Technology) and information environments. A thorough, all inclusive, risk analysis exercise needs to be conducted in business *and* supporting environments in order to develop an effective internal control system. Such an internal control system should reduce the exposure of risk and aid the safeguarding of assets. Indeed, in today's so-called information age, where business processes integrate the business and ICT environments, it is imperative that a unary internal control system be established, based on a holistic risk management exercise. To ensure that the enterprise, information and ICT environments operate free of the risks that threaten them, the risks should be properly governed. A model, EPiRISMM (Enterprise Information Risk Management Model) is proposed that offers to combine risk management practices from an ICT, information, governance, and enterprise perspective because there are so many overlapping aspects inherent in them. EPiRISMM combines various well-known standards and frameworks into one coherent model. By employing EPiRISMM, an enterprise will be able to eliminate the traditional segmented approach of the ICT department and thus eliminate any previous discontinuity in risk management practices.

TABLE OF CONTENTS

Chapter 1 INTRODUCTION 2
1.1 Background 2
1.2 Description of Problem Area 3
1.3 Problem Statement 4
1.4 Objective 4
1.5 Research Philosophy and Methodology 5
1.6 Proposed Layout of Dissertation 6
1.7 Summary 8
Chapter 2 TAXONOMY OF ICT RISK MANAGEMENT 10
2.1 Introduction 10
2.2 Risk in General 11
2.3 Why Risk Management? 17
2.4 What is the Management of Risk? 19
2.5 Risk Analysis 21
2.6 Risk Management 26
2.7 Risk Management from an ICT perspective 28
2.8 Conclusion 45
Chapter 3 CORPORATE COVERNANCE 46
3.1 Introduction 46
3.2 What is Corporate Governance? 46
3.3 Why Corporate Governance? 48
3.4 Learning from Other's Failures 49
3.5 Principles of Corporate Governance 51
3.6 Governance Regulations and Guidelines 53
3.7 Governance Roles and Responsibilities 59
3.8 Corporate Governance and Risk Management 66
3.9 Conclusion 67
Chapter 4 ENTERPRISE RISK MANAGEMENT 69
4.1 Introduction 69
4.2 History of Enterprise Risk Management 69
4.3 What is Enterprise Risk Management? 71
4.4 Components of ERM 71
4.5 Enterprise Risk Management Frameworks 73
4.6 Limitations to ERM 83
4.7 Conclusion 84
Chapter 5 ICT RISK MANAGEMENT: THE PROBLEM 86
5.1 Introduction 86
5.2 Why Information is Important 86
5.3 What is Information Security? 87
5.4 Information Security Guidelines and Regulations 89
5.5 The Evolving Dependency on Information 94
5.6 The Evolution towards the Information Age 96

5.7 Risk Management to Ensure a Quality Lifestyle....98
5.8 Risk Management from an Enterprise Perspective....101
5.9 Defects of Information Risk Management....107
5.10 Conclusion....107
Chapter 6 EPIRISMM: AN ENTERPRISE INFORMATION RISK MANAGEMENT MODEL....110
6.1 Introduction....110
6.2 EPiRISMM Objectives....111
6.3 EPiRISMM: The Conceptual Model....112
6.4 Employing EPiRISMM....120
6.5 Conclusion....120
Chapter 7 EPIRISMM: THE DETAILED MODEL....122
7.1 Introduction....122
7.2 Step 1: Selecting Relevant Standards, Best Practices and Guidelines....122
7.3 Step 2: Extracting and Combining Activities....124
7.4 Step 3: Applying Activities at Various Organisational Levels....128
7.5 Conclusion....140
Chapter 8 EVALUATING EPIRISMM....141
8.1 Introduction....141
8.2 Nature of the Case Study....141
8.3 Company XYZ Profile....141
8.4 Applying EPiRISMM at XYZ....143
8.5 Findings and Suggestions....145
8.6 Conclusion....146
Chapter 9 CONCLUSION....148
9.1 Background....148
9.2 Summary....148
9.3 Solving the Problem....150
9.4 Limitations of this Study....152
9.5 Future Research Directions....153
9.6 Epilogue....153

LIST OF FIGURES

Figure Page

Figure 1-1: Layout of Dissertation 7
Figure 2-1: Risk Discussion Flow 11
Figure 2-2: Taxonomy of Risk and Opportunity 17
Figure 2-3: Taxonomy of the Management of Risk 21
Figure 2-4: Risk Probability/Impact Matrix 26
Figure 2-5: A Summary of ICT Risk-Related Concepts 30
Figure 2-6: ICT Risk Identification Activities 34
Figure 2-7: Risk Management Strategy Selection 40
Figure 2-8: Risk Mitigation Questions 41
Figure 2-9: GTAG 1 - Classification 44
Figure 4-1: Treasury Board of Canada's Integrated Risk Management Framework 75
Figure 4-2: Grant Thornton ERM Framework 79
Figure 4-3: Grant Thornton ERM Risk Profile 79
Figure 4-4: The COSO ERM Framework 82
Figure 5-1: Evolving Dependency on Information 96
Figure 5-2: Risk Management along Evolution of Dependency on Information 97
Figure 5-3: Bodily Risk Management 99
Figure 5-4: Risk Management from an Enterprise Perspective 103
Figure 6-1: ICT and the Enterprise are Inseparable 112
Figure 6-2: The Enterprise and Governance Aspects are Inseparable 113
Figure 6-3: Governance and ICT Aspects are Inseparable 114
Figure 6-4: Relationship between Information, Governance, ICT and the Enterprise 114
Figure 6-5: Draft Cubical Model Preceding EPiRISMM 115
Figure 6-6: Pyramidical Model Preceding EPiRISMM 116
Figure 6-7: Top view of EPiRISMM 117
Figure 6-8: Management Levels 119
Figure 6-9: Three Dimensional Representation of EPiRISMM 119
Figure 6-10: The Steps in EPiRISMM 121
Figure 7-1: The Ansoff Matrix 132
Figure 7-2: Policy Hierarchy 134

LIST OF TABLES

Table Page

Table 2-1: Definitions for Risk, Opportunity, Chance and Uncertainty 17
Table 2-2: Information Security Controls.....42
Table 5-1: A Comparison of Risk Management from a Human and Enterprise Perspective..... 105
Table 6-1: EPiRISMM Acronym..... 110
Table 7-1: Enterprise Activities Identified in COSO ERM 124
Table 7-2: Governance Activities Identified in King II 125
Table 7-3: Information Activities Identified in ISO 27001 125
Table 7-4: ICT Activities Identified in ISO/IEC 13335..... 125
Table 7-5: Combination of ISO 13335, ISO 17799, King II and COSO ERM 126
Table 7-6: Levels of Management 128
Table 7-7: Activities from Table 7-5 Applied on those of Table 7-6 129
Table 7-8: Management of Risk Activities..... 137
Table 7-9: Monitoring Activities..... 139
Table 7-10: Communication Activities..... 139

ACRONYMS AND ABBREVIATIONS

ADB Asian Development Bank

AIMIC Association of Insurance Managers in Industry and Commerce

AIRMIC Association of Insurance Risk Managers in Industry and Commerce

ALARP As Low As Reasonably Practicable

ALE Annual Loss Expectancy

AS/NZS Australian Standard/New Zealand Standard

BCP Business Continuity Planning

BS British Standards

BSI British Standards Institute

CAATT Computer Assisted Audit Tools and Techniques

CACG Commonwealth Association for Corporate Governance

CCTA Central Computer and Telecommunication Agency

CEO Chief Executive Officer

CIA Confidentiality, Integrity, Availability

CIO Chief Information Officer

CNSS Committee on National Security Systems

COBIT Control Objectives for Information Technology

COSO Commission Of Sponsoring Organisations

CRAMM Risk Analysis and Management Methodology

CRC Chemical Rubber Company

DM Deutche Mark

EPiRISMM Enterprise Information Risk Management Model

ERM Enterprise Risk Management

EVA Economic Value Added

FMECA Failure Modes and Effects Criticality Analysis

GAAP Generally Acceptable Accounting Practices

GMITS Guidelines to the Management of Information Technology Security

HMSO Her Majesties Stationary Office

HAZOPS Hazard and Operability Studies

ICAEW Institute of Chartered Accountants in England and Wales

ICT Information and Communication Technology

IEC International Electrotechnical Commission

IRM Institute for Risk Management

ISACA Information Systems Audit and Control Association

ISBN International Standard Book Number

ISMS Information Security Management System

IL Illinois

IRMI International Risk Management Institute

ISO International Organisation for Standardisation

IT Information Technology

ITGI Information Technology Governance Institute

ITIL Information Technology Infrastructure Library

IWS Information Warfare Site

JSE Johannesburg Stock Exchange

KPI Key Performance Indicator

KPMG Kleinveld, Peat, Marwick, Goerdeler

LLC Limited Liability Company

LRAM Livermore Risk Analysis Methodology

LSE London Stock Exchange

MD Managing Director

NIST National Institute of Standards and Technology

OGC Office of Government Commerce

ROE Return on Equity

ROI Return on Investment

RR Residual Risk

SEC Security and Exchange Commission

SOX Sarbanes-Oxley Act

SP Special Publication

SWOT Strengths, Weaknesses, Opportunities, Treats

TR Technical Report

UCL University College London

UK United Kingdom

UPS Uninterruptible power supply

URL Universal Resource Locator

USA United States of America

US United States

Section 1: Introduction

Chapter 1

INTRODUCTION

1.1 Background

"Information is power, but it is pointless power if hoarded. Power must be shared for an organisation or a relationship to work" (Dupree, 1989). Information and communication technology (ICT) enables such power sharing within an enterprise. Thus, ICT plays a pivotal part in enterprises today, and it will continue to play an even more important role in the future (von Solms, 1998). Organisations are also becoming more and more dependent on information being shared between them, such as used in supply chains.

"Information is power? No, but … Organised information is strength. Accurate information is essential. Up-to-date, new information is valuable. Communication is vital. Ongoing communication is organisation. Intentional communication is strategic. Expanding communication is growth. Many-to-many communication is vibrant. Therefore … intentional, ongoing, expansive, many-to-many communication, within the context of organised, accurate, up-to-date information, is power" (Clift, 1999). What this comes down to is that information offers no power to an organisation, if it is inaccurate and error prone, in the wrong hands and unavailable when needed. There are various risks that may influence information and prevent the right information arriving at the right place and at the right time to empower an organisation. These risks need to be managed.

The early Chinese general, Sun Tsu, commented in his book, *The Art of War* that "if you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained, you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every

battle." This highlights the fact that one should know oneself as well as the enemy in order to protect oneself from harm.

1.2 Description of Problem Area

Risk management can be seen as the war described by Sun Tsu. It consists of numerous battles against the enemy in order to protect one's assets against harm. In preparation for war, one needs to consider oneself and one's enemy. This preparation can be seen as risk analysis; the activity preceding risk management. Together, risk analysis and risk management are described as *the management of risk* (British Standards Institution, 1991).

Various techniques have been developed over the years to manage risks in different domains. People within the various domains, of course, see risks differently, depending on their domain and their background. With the development of these strategies, some of the overall focus of what risk management is ultimately striving for, has been lost. This is due to the level of specialisation and evolution of the various fields, especially pertaining to ICT and information.

The management of risk from an ICT perspective is an example of evolution over the years. Initially, with the introduction of computers, only physical security had to be considered. Enterprises were not as dependent on computer infrastructure as today, because all operations were performed in batch. Nowadays, risk management for information and ICT must be considered together within the larger enterprise environment.

Information is integrated into all business processes, and the risks associated with normal business, particularly with regard to financial aspects, cannot be divorced from information-related risks. Therefore, organisational risk management requires a single, integrated approach to the process of managing information, as well as business, financial and other related forms of risk. To integrate all organisational efforts of risk management effectively, it is important to study the origin of risk and risk management.

1.3 Problem Statement

The business environment and information technology are bound together by information. For this reason, it is imperative that risk management and its underlying terminology are synergised in both the business and ICT worlds. A thorough risk analysis needs to be conducted in business and supporting environments in order to develop an internal control system. Indeed, in today's so-called information age, where business processes integrate the business and IT environments, it is imperative that a unary internal control system be established. Owing to the nature of risk terminology, it is almost impossible for people in the ICT and business worlds to communicate effectively.

The main problem addressed by this research project is defined as:

> A major problem experienced in the business environment today is that enterprise risk is hard to manage effectively, because business and information-related risks are not congruently aligned with risk management practices.

The following secondary problems can be derived from the main problem, and also need to be addressed:

- What are the views on risk within various disciplines?
- What factors influence risk management in an enterprise?
- How can these influences be represented to reflect an integrated information risk management approach?
- How can this representation be used to manage information risks holistically?

1.4 Objective

The primary objective of this study is to develop a model to integrate risk management practices in today's business and information environments and ultimately assist in the management of information related risks.

The following secondary objectives have to be addressed:

- to conduct a contextual literature survey on related risk paradigms;
- to determine what factors influence risk management in an enterprise;
- to represent these factors to reflect integrated information risk management; and
- to employ this representation to holistically manage information-related risks in the enterprise.

1.5 Research Philosophy and Methodology

This dissertation is considered to fall in the social phenomena domain, because information systems as well as information security will usually involve people. Thus, the meaning of the study, the qualitative values rather than the measurement, or quantitative values, are emphasised. Therefore, this research dissertation and its philosophy will be predominantly phenomenological and interpretive oriented. Thus, the research methods will consist of literature studies, modelling and arguing. To provide a more balanced research offering, a case study will also be conducted at the end.

The methodology will consist of a broad literature study to gain a better understanding of risks and the management thereof from various discipline-oriented viewpoints. The literature studied was obtained from various journals, books, recent standards and acts, and any other material that is relevant and of acceptable quality.

When this broad literature study is completed, and various problem areas identified, a more focused literature study is conducted. This study concentrates on the differences and similarities of the various discipline-oriented viewpoints, where after the influences of information-related risk management within an enterprise is identified.

Hereafter, a model is developed to ensure that risks can be managed in a holistic way. The soundness of the model is tested by means of a case study and reasoning. However, a complete case study is not undertaken. It would be unwise to conduct a case study on a company, as this in itself would be a major risk. A paper was prepared and forwarded to an international journal for publication.

1.6 Proposed Layout of Dissertation

The layout of the dissertation is depicted in Figure 1-1. **Chapter 1** offers a background to the study in order to delineate the problem. The problem was further broken down into secondary problems, which in turn were translated into a main objective and various secondary objectives. **Chapter 2** addresses risk and risk management, both from a general perspective and an ICT perspective. The history of risk management, perceptions of risk, as well as various techniques to manage risk are also discussed. In **Chapter 3,** corporate governance is addressed. In the discussion on corporate governance, three corporate failures and various corporate governance regulations are highlighted. Chapter three concludes with a parallel being drawn between corporate governance and risk management and how corporate governance relates to risk management. **Chapter 4** discusses the concept of enterprise risk management (ERM). In the discussion on ERM, its history is represented, along with various ERM frameworks, similar to the discussion on the various regulations in chapter 3. Chapter 4 is concluded with an overview of the limitations of ERM. **Chapter 5** discusses general information security, also highlighting the important publications pertaining to information security. Thereafter, the importance of an integrated approach to information risk management is reinforced by making use of an analogy that compares the enterprise with the human body. **Chapter 6** builds on chapter 5 and shows how the aspects discussed in chapters 2 through 5 come together and influence information risk management. The relationship is indicated between these aspects, i.e. information, ICT, corporate governance and the enterprise. This is done by making use of a model that is broken down into three steps. The model is expanded in **Chapter 7** where various activities are identified to holistically manage information-related risks by making use of the three steps from chapter 6. These activities were tested in **Chapter**

8, where they were used in a case study to identify possible improvements. **Chapter 9** offered the conclusion.

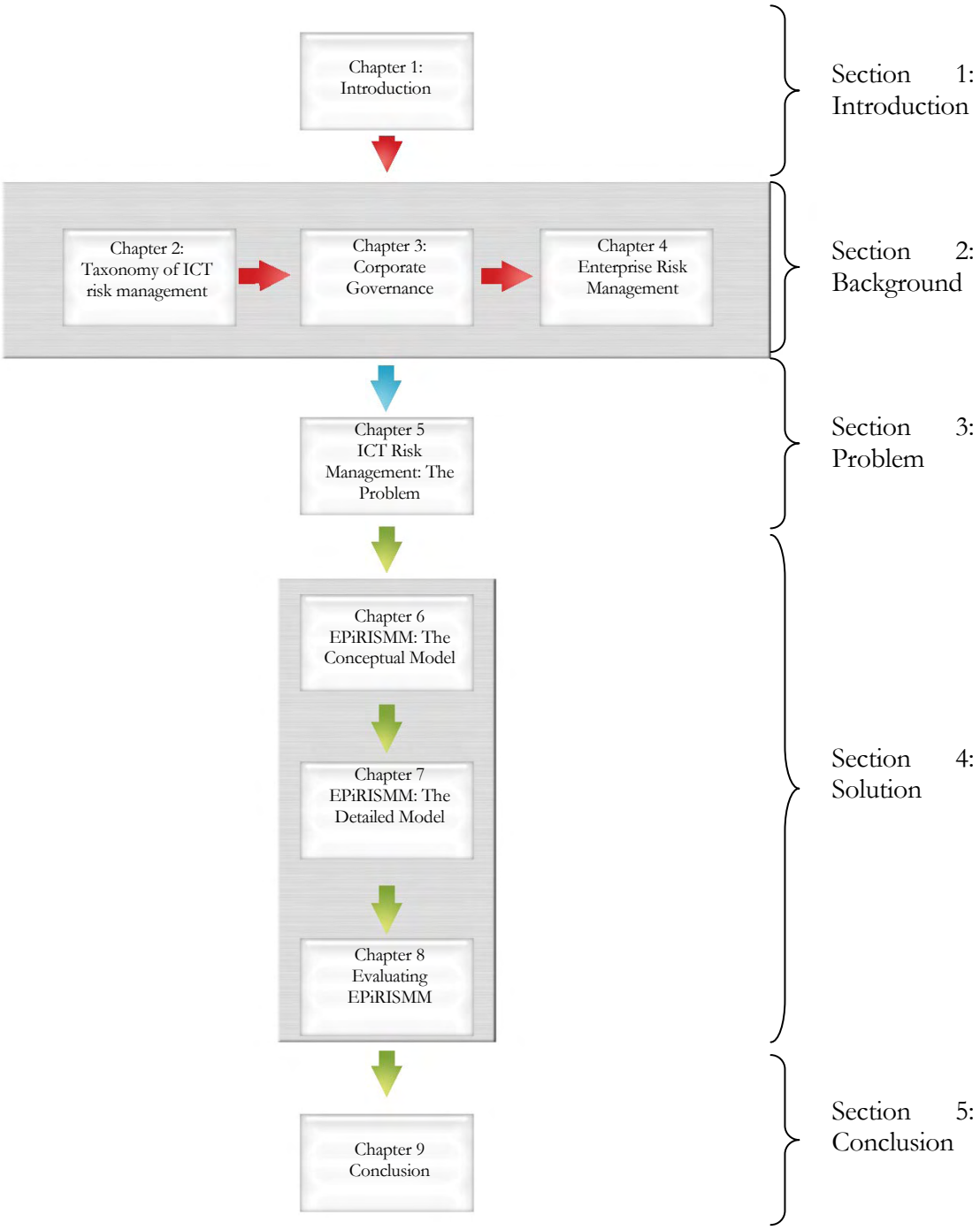


Figure 1-1: Layout of Dissertation

1.7 Summary

This chapter introduced the fact that information is pivotal and omnipresent throughout enterprises. Because information is so important and integrated in enterprises, the information risk management approach should be an all-inclusive one. This is emphasised in the problem statement that to manage information-related risks effectively, an integrated approach is needed. Because of this problem, the objective of this study is to develop a means to integrate information-related risk management practices in the enterprise. This will be achieved by following the research philosophy and methodology discussed in Section 1.5. The next chapter, Chapter 2, will begin to offer a background to the overall study, as discussed earlier.

Section 2: Background

Chapter 2

TAXONOMY OF ICT RISK MANAGEMENT

2.1 Introduction

Chapter 1 stated that information and the supporting information and communications technologies (ICT) can no longer be divorced from the business environment. Information is the "lifeblood" of all business processes (Halliday, Badenhorst, & von Solms, 1996). Therefore, business and information risks need to be managed in an integrated way. Risk management, from a business and information technology point of view, encompasses different processes. The result is that different terminologies and interpretations have developed over time. When considering the way in which all business and information-related risks are currently interpreted, it is important to eliminate the terminologies and conceptual interpretations that cause confusion and also ensure the alignment of the technology with the business.

The first objective of this chapter is to offer the contextual background on risk and risk management. Because the term 'risk' has different meanings to different audiences, a contextual definition will be offered as well as how this dissertation will interpret the term. The second objective of this chapter is to elucidate risk management as a term and as a concept, both of which are also interpreted in various ways. The last objective of this chapter is to put forward an ICT perspective on risk and risk management.

The layout of this chapter will follow the outline of the objectives, firstly discussing risk in general by looking at various definitions, and discussing how the term has changed over time. A description of the sources and areas of risk in the business environment is also highlighted. The management of risk is then discussed, and the origin of this term is investigated. After establishing the meaning of risk and risk management in general, risk and risk management from an information and communications technology

perspective are discussed. The flow of the section on ICT risk and its management will follow the same flow as the section on general risk, as depicted in Figure 2-1.

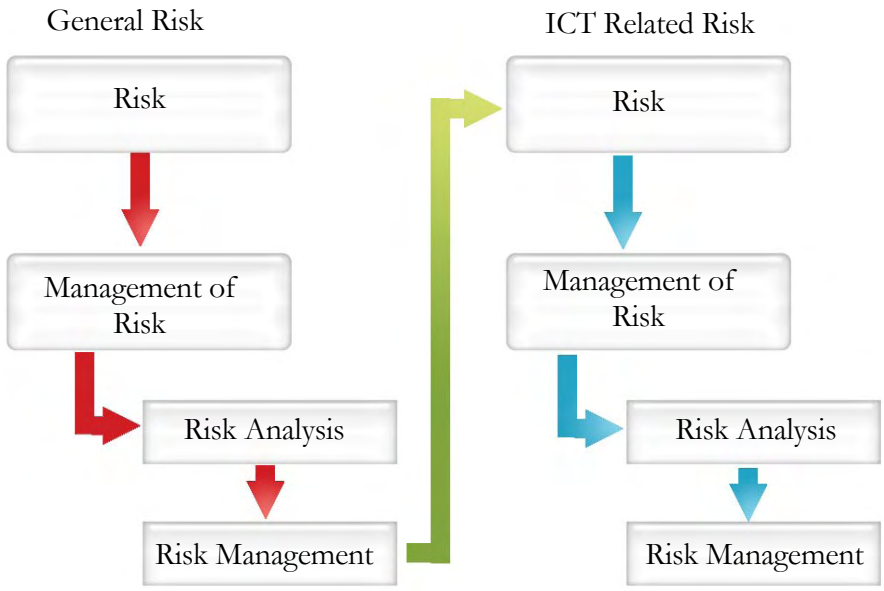


Figure 2-1: Risk Discussion Flow

2.2 Risk in General

The term risk is used by numerous individuals, from professionals to laymen. However, the usage and interpretation of this term appears to differ widely. From the beginning, the general meaning has changed significantly. According to Harding (1998), the formal, technical meaning of the word refers to "[a] combination of the probability, or frequency, of occurrence of a defined hasard and the magnitude of the consequences of the occurrence: how often is a particular potentially harmful event going to occur, [and] what are the consequences of this occurrence?" To clarify understanding of the term risk, a brief overview of its historical meaning should be examined.

Douglas (1990) traced the origin of the term risk, back to the 17th century when risk was associated with the mathematics of gambling. Risk was referred to as a combination of probability and degree of possible gains or losses. During the 18th century, marine insurance viewed risk as neutral, where both gains and losses were

taken into account. During the 19th century, the concept of risk emerged in economics, and people were considered to be opposed to risk-taking. In the 20th century and today, risk is also mostly perceived as negative.

Evidently, the definition of "risk" has varied over time. This variation is summarised by Graubard (1990) as follows: "It is perfectly obvious that the concept 'risk' has taken on wholly new dimensions in recent decades and is today being reflected on in ways that would have been almost inconceivable even a few years ago. The older idea, that risk is essentially a wager, which individuals take in the hope of gaining something significant or substantial, has almost disappeared from common parlance. Risk today is conceived principally as danger…"

There are two schools of thought regarding the outcomes of risk today. The one primarily sees risk as negative, the other argues that there is a possible upside to risk and that risk should not only be considered negatively.

"The possible loss of something of value" (Blomkvist, 1987), is one of numerous definitions of risk that indicates that it is a negative concept and does not have an upside. Another more aggressive definition indicates that risk is a "catastrophe in its latent form" (Friedman, 1987). Merkofer (1987) provides a definition of risk that indicates that various outcomes are possible and not all of these outcomes are negative. Adams states that risk "is defined, by most of those who seek to measure it, as the product of the probability and utility of some future event" (1995). Where Adams states "those who seek to measure it", he also refers to scientists of the natural sciences paradigm. These various views will be discussed briefly.

The Collins Cobuild English Language Dictionary (1987) defines risk as "a possibility that something unpleasant or undesirable might happen … [if] you take a risk, you do something which you know might be dangerous or have unpleasant consequences." Furthermore, it states that to achieve a goal, a risk may be necessary. From these definitions, it would seem that while risk-taking appears negative, there are also possible rewards.

Another argument is that risk may start with uncertainty (COSO ERM, 2004a; Wixley & Everingham, 2002). Uncertainty, which is defined as "something that nobody can predict or guarantee" (Encarta Reference Library, 2005d), may be viewed both positively and negatively. A positive aspect is that opportunities may be offered that potentially enhance value, while the negative side is that risk may potentially erode value. Wixley and Everingham (2002) further states that "[s]uccess in business and in life results from exploiting opportunity but managing risk". The King Report on corporate governance (King II, 2002) defines commercial enterprise as the undertaking of business for reward. To have a successful business, a balance between risks and opportunity must exist.

The Royal Society Study Group (1983; 1992) defined risk as "the probability that a particular adverse event occurs during a stated period of time, or results from a particular challenge". This statement was supported by the British Standards' definition of risk as "a combination of the probability, or frequency, of occurrence of a defined hazard and the magnitude of the consequences of the occurrence" (British Standards Institution, 1991). This definition was included in the Royal Society Study Group's report (Frosdick, 1997).

As highlighted earlier, layman and scientists have different perceptions of risk. Similarly, there are various arguments between scientists from various domains regarding risk. The scientists in natural sciences, i.e., physics, chemistry, biology, and the theoretical sciences, i.e., philosophy and mathematics, and applied sciences, i.e., engineering, attempt to assign numerical values to risk. Frosdick (1997) states that "the engineering paradigm is one of quantification". For quantification, numbers are calculated by making use of probabilities and information extracted from a databank. The information in the databank is captured over time. This databank contains information on failures and reliability. Thus, calculations of risk are based on an objective, systematic and non-biased approach (Kirkwood, 1994).

Scientists from the social sciences, however, i.e., anthropology, psychology and cultural studies have a different view. They argue that risk is socially constructed and means

different things to different people (Royal Society, 1992). The Royal Society's report elaborates on this by stating that "a particular risk or hazard [means] different things to different people in different contexts". It is agued by psychologists that layman only perceive the consequences of risk and do not consider the frequency (Frosdick & Odell, 1996). Certain risks are "exaggerated or minimised according to the social, cultural, and moral acceptability of the underlying activities" (Covello & Johnson, 1987). People perceive risks based on personal experience, memory and other factors (Garvin, 2001; Spangler, 1984). Furthermore, people adapt the levels of risk they are willing to accept according to their comfort levels (Botterill & Mazur, 2004). Adams (1995) calls this a "risk thermostat". This risk thermostat refers to the concept of risk homeostasis.

Risk homeostasis can be compared to homeostasis in the human body where the normal core body temperature is 37°C. The human body maintains this temperature despite variations in the surrounding temperature. Risk homeostasis can be demonstrated through the example of car accidents when the seatbelt regulation was introduced. Adams argues that not only the drivers of the cars should be considered, but that pedestrians and other road users should also be taken into account. Drivers might take more chances because they are feeling safer strapped in with the seatbelt, and the other road users could be affected.

It becomes apparent that the term risk may be interpreted in different ways, based on the preceding discussion. One aspect became apparent; risk is directly related to the context wherein it is perceived. Various definitions of risk have been discussed to elucidate all interpretations relating to specific contexts. This dissertation will interpret the word *risk* as a negative aspect. However, risk should not be mentioned without considering opportunities, the upside of risk within context. A good example of the use of the word, risk, is "you risk your life's savings by investing in the stock exchange". This indicates that there is a chance that you might lose your money, but there are possible rewards. The risks that an enterprise faces are natural in various organisational sections. These are discussed in the next section.

Areas of risk in an enterprise

While risk may be interpreted in various ways, risk in an enterprise is divided into strategic, financial, operational and hazard risk in the business environment to offer common ground for risk discussion. Some risks may fit into more than one of these categories (Darlington, Grout, & Whitworth, 2001). Darlington *et al* (2001) state that risk in each of these four categories may again be divided into internal and external risks.

Operational risk is "[t]he risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems or from external events" (Basel II, 2006). Examples of operational risk include process risk, IT risk, control system risk, human capital risk, health and safety risk and compliance risk.

Financial risks relate to the negative aspect of having too much debt (Ketz, 2003). If an organisation has debt, external factors come into play such as fluctuating exchange and interest rates. Examples of financial risk include economic risk, market risk and credit risk, as well as various related operational risks (Darlington *et al.*, 2001).

Hazard risks have a genuine negative connotation. Examples of hazard risk are property risk, such as theft and vandalism, liability risk, such as lawsuits, environmental risks, such as liability for pollution, natural disasters and political risks such as war and terrorism (Darlington *et al.*, 2001).

Strategic risks include mergers and acquisition risk, business risk, competitor risk, brand risk, legal risk and new opportunity risk (Darlington *et al.*, 2001). Strategic risks are connected to the decisions being made in organisations as they are based on questions being asked for the various risks. For example, customer risk may result in the question "what are the likely demographic and demand changes?" Therefore, it can be argued that strategic risks have a definite upside to them.

> Notwithstanding the category wherein a risk may fall, in general, it can be argued that all risk is socially constructed. While scientists from the natural and theoretical sciences attempt to measure risk, those from the social sciences consider them as only having their own perception on risk. Slovic (1999) summarises risk not to "exist 'out there', independent of our minds and cultures, waiting to be measured. Instead, human beings have invented the concept *risk* to help them understand and cope with the dangers and uncertainties of life. Although these dangers are real, there is no such thing as 'real risk' or 'objective risk.' The nuclear engineer's probabilistic risk estimate for a nuclear accident or the toxicologist's quantitative estimate of a chemical's carcinogenic risk are both based on theoretical models, whose structure is subjective and assumption-laden, and whose inputs are dependent on judgement."

In summary, Figure 2-2 expresses the taxonomy of risk and opportunity. Table 2-1 offers definitions of the terms used therein. Uncertainty can be divided into risk and opportunity. Risk is the negative side of uncertainty, and opportunity the positive side. Chance is an aspect very closely related to uncertainty, and can be defined as the "likelihood that something will happen" (Encarta Reference Library, 2005c). Therefore a risk can be defined as the likelihood that something can go wrong, and an opportunity can be defined as the likelihood that something advantageous might happen.

Risk, the downside of uncertainty, needs to be managed to minimise negative outcomes and enable an enterprise to pursue opportunities. This is called risk management and will be discussed in the next section.

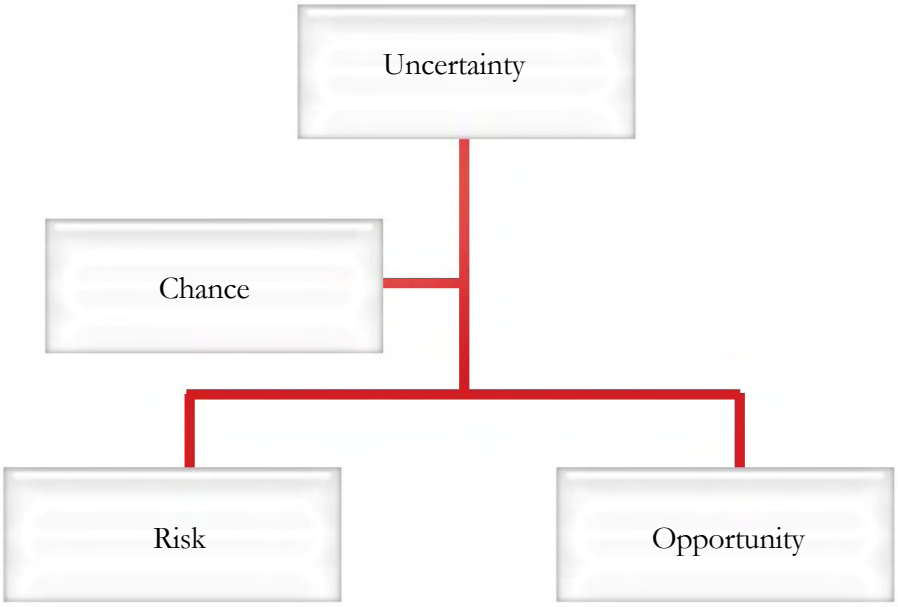


Figure 2-2: Taxonomy of Risk and Opportunity

Table 2-1: Definitions for Risk, Opportunity, Chance and Uncertainty

Uncertainty	Something that nobody can predict or guarantee
Opportunity	A chance, especially one that offers some kind of advantage
Risk	Chance of something going wrong
Chance	Likelihood that something will happen
Thus: Opportunity	The likelihood that something advantageous might happen
Thus: Risk	The likelihood of something going wrong

2.3 Why Risk Management?

Risk is omnipresent; it is imbedded in every aspect of business. Risks should be managed to ensure that all opportunities are taken. However, an enterprise needs to

know what risks to manage before risks can be managed. Lichtenberg (1742-1799) stated that "once we know our weaknesses, they cease to do us any harm." In order to gain a better understanding of risk management, the history thereof will be discussed next.

A brief history of risk management

Terry Simister (2000) from the Institute of Risk Management states that risk management was introduced during the 1950s in the USA. Markowitz indicated in 1952 that is it mathematically possible to link risk and potential return (Bernstein, 2001). According to Hunt, a Harvard Business Review article was published in 1956 that stated how a risk manager could be employed to lessen business losses. However, this management position was directly related to the role of insurance manager. The use of the term "risk management" was only introduced in the UK in 1969. Doug Barlow gave the first "authoritative" presentation on the subject of risk management. The Association of Insurance Managers in Industry and Commerce (AIMIC) recognised that they are risk managers as well and became AIRMIC, the Association of Insurance Risk Managers in Industry and Commerce (Simister, 2000). This led to numerous insurance managers changing their titles to "Risk Managers" (Simister, 2000). A somewhat different perspective is given by Borodzicz (2005). Borodzicz argues that risk management and assessment has indeed matured as a scientific venture by the mid twentieth century, especially in engineering, physics and mathematics (Borodzicz, 2005).

In the seventies, the business environment started to recognise the benefits of risk management. However, the adoption of risk management was mostly limited to financial organisations. Non-financial organisations did not keep up with their financial counterparts by developing their own risk management functions and practices. Non-financial organisations only started developing their own practices in the nineties (Hunt, 2001).

Risk management in the eighties evolved from country risk to political risk, according to Hunt (2001). This happened because of the Iranian revolution and political instability worldwide. However, in the late eighties, stability returned, and risk management practices were still focused on the insurance industry (Hunt, 2001).

The importance of risk management began to grow and various organisations started offering assistance and advice in this regard. Risk management was considered a profession by 1986 (Simister, 2000). The need to "set standards for qualifications and grant designatory letters" led to the Institute of Risk Management (IRM) opening its doors in March of 1986 (Simister, 2000).

At the beginning of the nineties, risk management was synonymous with buying insurance and financial hedging schemes to minimise losses (Hunt, 2001). Today, risk management is pivotal to any organisation's decision-making as it enables stable, continuous business operations.

Simister (2000) argues that after 30 years, there is still no clear understanding about what "risk management" actually means. While Simister spoke mainly of risk management in the financial and insurance context in his discussion, risk management is not limited to this as Borodzicz indicated. Another industry that has developed its own risk management methodologies is the engineering discipline. However, the methodologies used in engineering differ substantially from those used in financial industries.

Despite these differences, a pattern emerges: first risks are identified and prioritised, and then actions are taken to minimise the effect of the risks. This pattern that has been observed will be used in the next section to discuss the management of risk.

2.4 What is the Management of Risk?

Clearly risk is an omnipresent phenomenon that humans created to help us understand and predict our surroundings. The meaning of the term, risk, as well as the term, risk

management, has evolved over time. Today confusion still exists over what the term actually means. This section discusses what the term currently means and that risk management plays a pivotal role in organisations to assist managers in making decisions.

The British Standard Institute (BSI) distinguishes between risk management as a term and a concept. The BSI argues that the term refers to "the process whereby decisions are made" (British Standards Institution, 1991), while the concept refers to "the overall subject area concerned with hazard identification, risk analysis, risk criteria and risk acceptability". Such duality could lead to ambiguity and uncertainty. The British Government Centre for Information Systems provides a manner to distinguish between "risk management" and "the management of risk". Risk management "refers to planning, monitoring and controlling activities which are based on information produced by risk analysis activity", while the management of risk "describe the overall process by which risks are analysed and managed" (Scarff, Carthy, & Charette, 1993). This approach, i.e., dividing the management of risk into risk analysis and risk management, will be followed in this dissertation. A similar definition is given by the Royal Society, which defines risk management as "the making of decisions concerning risks and their subsequent implementation, and flows from risk estimation and risk evaluation" (Royal Society, 1992).

From these definitions, it can be concluded that the management of risk can be divided into two sections, risk analysis and risk management. The activity preceding risk management i.e., risk analysis, includes risk identification, risk estimation and risk evaluation all put together (Frosdick, 1997). Frosdick argues that risk analysis and risk assessment are synonymous (Frosdick, 1997). All of these are summarised in Figure 2-3, and will be discussed in more detail in subsequent sections. In addition, risk management can be sub-divided into risk control (also referred to as internal control) and risk monitoring (Bandyopadhyay, Mykytyn, & Mykytyn, 1999).

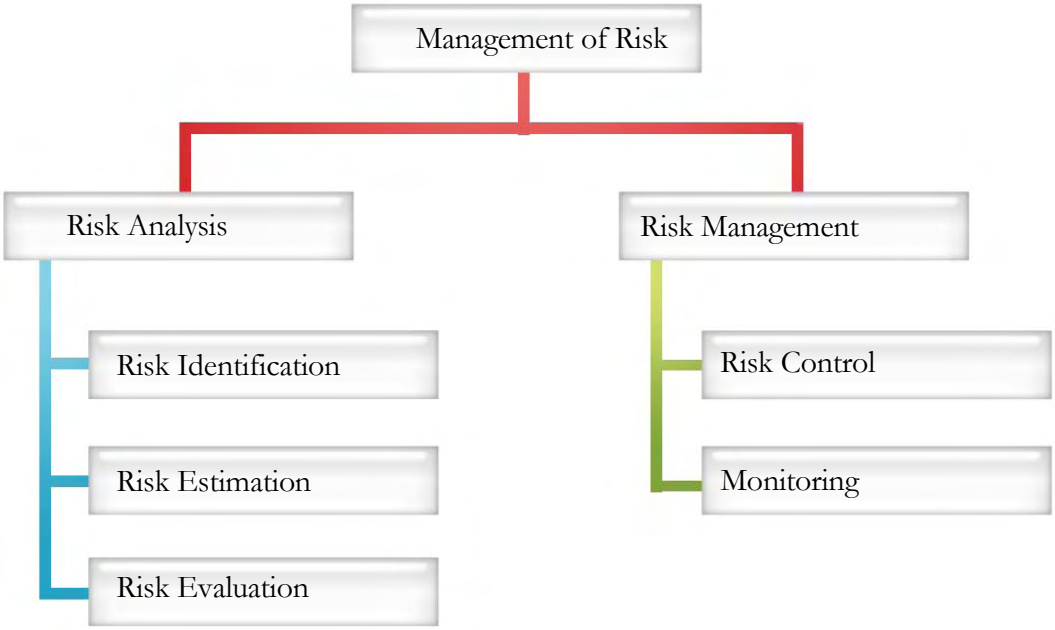


Figure 2-3: Taxonomy of the Management of Risk

2.5 Risk Analysis

This section will discuss the components of risk analysis as part of the management of risk. Refer to Figure 2-3.

2.5.1 Risk identification

Tchankova (2002) states that the first stage of risk analysis, which forms part of the greater management of risk, is **risk identification** (Figure 2-3). This is used to determine and uncover possible risks (Tchankova, 2002). Tchankova suggests that risk identification can be divided into four parts. These include the sources of risks, hazard factors, perils and exposures to risk. To identify risks, it is important to consider the sources of risk, which include acts of God, the social environment, the political environment, and the operational environment. These will all be discussed in more detail shortly. "*Hazard* is a condition or circumstance that increases the chance of losses or gains and their severity" (Tchankova, 2002), while *peril* is an aspect related to risk that has a negative

outcome. The *resources exposed to risk* are those assets of the enterprise that are facing the risks.

These components of risk identification are clarified in the following example:

In a hospital, some blood is stored in a special laboratory for testing. The source of the risk would be the internal environment, while a hazard may be human error. Peril is possible contamination, while the resources exposed to the risk are the hospital staff and well as the hospital's reputation.

Sources of risk

Up to now, the definition of risk has been discussed without mention of the sources of risk. Williams, Smith and Young (1998) argue that a classification scheme that covers more than merely social, physical and economic sources of risk is needed (Tchankova, 2002). This extended classification scheme includes physical, social, political, operational, economic, legal and cognitive environments.

Acts of God, or natural disasters, such as flooding, landslides, earthquakes, and lightning are sources of risk that stem from the **physical environment** (Tchankova, 2002). It is beyond the capability of humans to avoid these. However, to a certain extent, humans have learnt to predict when this type of risk might occur. This helps humans to be prepared when it does.

Risk in the **social environment** includes the "changes in people's values, human behaviours and state of social structures" (Tchankova, 2002). Such changes could lead to strikes, riots and social discontent. The media in this day and age may be a catalyst to risk in the social environment, and an enterprise, or even a country, could be at serious risk of a negative economic impact.

All countries experience risks from the **political environment**. A country's ruling party could change legislation and thereby influence the way businesses operate (Tchankova, 2002). Examples of such changes may include the changing

of taxation systems (Tchankova, 2002), the scrapping of import duties or even free trade agreements at a global level.

In an organisation, operational activities also generate risks. All workers are at risk in a company and could experience physical harm from a variety of sources, from a chair breaking to a fire in a mineshaft. These risks are classified as **operational environment** risks (Tchankova, 2002).

Once, an individual country's political environment would barely influence the **economic environment** (Tchankova, (2002). This seems to have changed recently as the global economic environment is in the hands of a few great countries. Tchankova (2002) states that globalisation should be considered separately. This type of risk affects economic recession and depression globally. At local level, interest rates and credit policies could also be affected (Tchankova, 2002).

Risk may also arise in a **legal environment,** for example, changes in legislation (Tchankova, 2002). In the global environment, countries have different legal requirements which increases the complexity of doing business internationally (Tchankova, 2002).

Lastly, the **cognitive environment** is the source of risks caused by people's understanding of the world around them. When people with different perceptions interact, differences could lead to risks.

Various risk identification methodologies and techniques have been developed to assist people involved to spot the risks accurately and timeously. The first such technique is **brainstorming**. This involves a group of people thinking about which risks are likely to occur (Schwalbe, 2002). The list of risks that is generated is then evaluated at a later stage during risk analysis. Another risk identification technique is the **Delphi technique**. This employs experts to reach consensus by means of systematic, anonymous and interactive inputs (Schwalbe,

2002). **Interviewing** is also a risk identification technique that enables the collection of information via face-to-face, telephone or even other types of electronic discussions (Schwalbe, 2002). Alternatively, a **SWOT** (strengths, weaknesses, opportunities and threats) **analysis** can also be used to identify various risks based on internal and external aspects. **Checklists** may be based on past experience or best practice in an industry (Marchewka, 2003). One negative aspect regarding checklists may be that they provide a false sense of security (Marchewka, 2003). Another technique is hazard and operability studies (**HAZOPS**), which is brainstorming performed by a team of interdisciplinary experts. Failure modes and effects criticality analysis (**FMECA**) is unlike HAZOPS in that it only uses one expert. Finally, **event** and **fault** trees can be used to indicate causes and consequences of failures respectively (Frosdick, 1997).

2.5.2 Risk estimation

Risk estimation is the next step in risk analysis (Figure 2-3) and involves assigning a value to a risk. Risk estimation can be quantitative or qualitative. Quantitative risk estimation involves measuring risks using mathematical and statistical tools. On the other hand, qualitative risk estimations make use of adjectives to describe the risks.

Qualitative risk estimation techniques include calculating risk factors using probability/impact matrices, top-10 risk item tracking and expert judgement (Schwalbe, 2002). A prioritised list of risks is created by calculating risk factors by using **probability or impact matrixes** (Figure 2-4). Risks are often classified into two dimensions: namely probability and impact (Schwalbe, 2002). Both the probability and consequence can be portrayed as being high, medium or low. Risks are then classified into high probability high impact, high probability medium impact, etc to low probability low impact (Schwalbe, 2002). Variations of this approach exist as well where numbers are assigned to high, medium and low, where after risks are ranked (Schwalbe, 2002).

Top-10 risk item tracking not only facilitates risk identification but also sustains risk awareness. Periodic risk reviews are held which indicate each of the risks' current ranking and previous ranking, as well as a risk resolution summary (Schwalbe, 2002). **Expert judgement** is the last qualitative risk estimation technique that will be discussed. Enterprises rely on experts to make decisions regarding the risks based on their knowledge and experience.

On the other hand, examples of two quantitative risk estimation techniques are decision trees and simulation (Schwalbe, 2002). The first, **decisions trees,** assists in making decisions regarding uncertain future consequences by making use of diagrams. The diagram consists of various branches of a tree, with each branch assigned a numeric value of the estimated probability. **Simulation** is a more advanced technique that makes use of a model that simulates various outcomes. A computer is employed to simulate the input of a given model numerous times and thereafter produces statistical results that are used in making risk decisions.

2.5.3 Risk evaluation

The final step in risk analysis is **risk evaluation** (Figure 2-3). All risks are considered during risk evaluation. Decisions are made regarding the identified risks by using the risk estimation results (Humprheys, Moses, & Plate, 1998). The objective of risk evaluation is to decide which risks should be managed. These decisions are based on the overall risk appetite of the enterprise, i.e., the level of risk the organisation is willing to accept. The risk appetite is decided on by the highest management levels of the enterprise, i.e., the board of directors (King II, 2002).

Risk criticality matrixes (Similar to Figure 2-4) and similar techniques are used to evaluate risks that have been identified and estimated by means of FMECA or event- or fault-trees. The various risks are marked on a chart, which again makes use of probability and consequence (Frosdick, 1997). The relative positioning between the risks are noted. Risks are prioritised and an acceptable threshold is

established by making use of the ALARP (as low as reasonably practicable) principle (Frosdick, 1997).

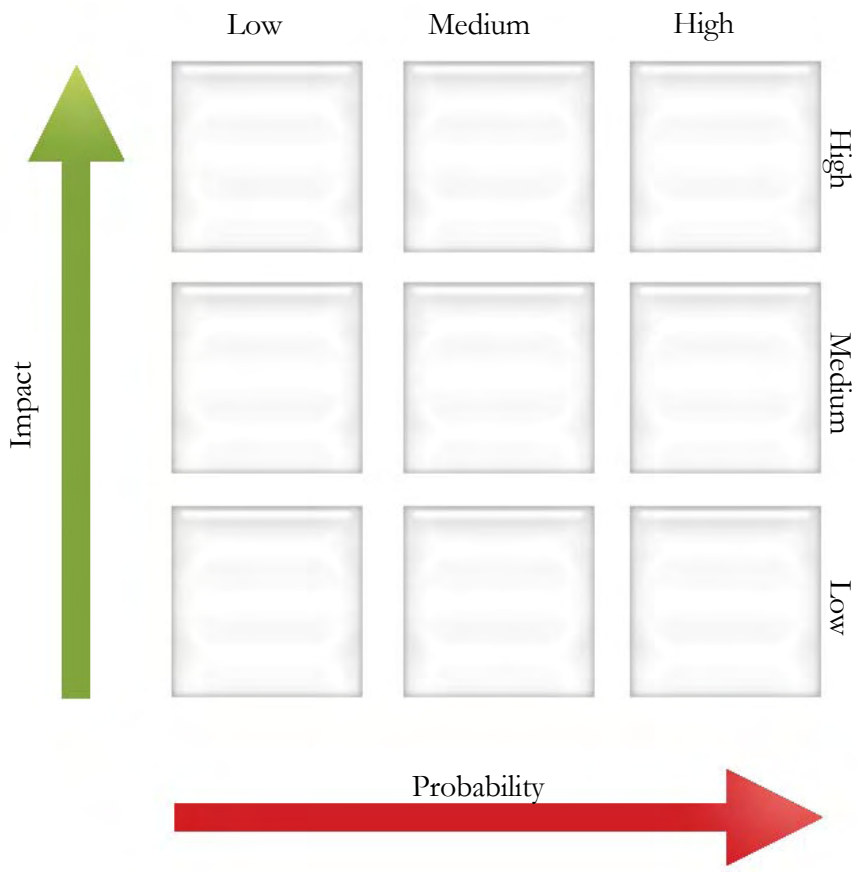


Figure 2-4: Risk Probability/Impact Matrix

Cost effectiveness and cost benefit analysis are used to evaluate risks by looking at the costs involved. The cost of the risk materialising and the probability thereof are compared to the cost of controlling the risk.

2.6 Risk Management

After all the risks have been analysed, i.e., identified, estimated and evaluated, actions should be taken to ensure that potential harm is minimised and opportunities are pursued (Figure 2-3). Depending on the risk and the enterprise's risk appetite, various

strategies can be followed. Some of these strategies include acceptance, mitigation, transference and avoidance.

A **risk avoidance** strategy attempts to stay away from all risks (Schwalbe, 2002). The enterprise does not attempt to address any risks and avoids them totally. The downside of this strategy is that possible opportunities may be lost. **Risk transference** attempts to shift the responsibility and consequences to a third party. An example of risk transference is transference to an insurance company. A **risk mitigation** strategy attempts to reduce the impact of the risk or reduce its probability. While such an approach might seem reactive, i.e., only attempting to mitigate the impact after the risk has been detected, some thorough proactive planning is needed. **Risk acceptance** means that an enterprise accepts the consequences of a risk should it occur (Schwalbe, 2002). The organisation attempts to absorb all the consequences of the risks. To make such a decision, a technique, such as cost benefit analysis, may be implemented.

Each of these risk management techniques is discussed again in a subsequent section providing insight from an ICT perspective.

An enterprise may implement any combination of these risk management strategies at a time. For example, some risks may be small, and the enterprise may choose to accept them. However, others may be outside the enterprise's scope; therefore, risk transference through insurance policies may be implemented.

Risk monitoring is the final step in the management of risk. During risk monitoring, risks are constantly reviewed and analysed, and actions are taken to ensure the risks do not exceed the risk appetite of the enterprise. Continuous risk monitoring also serves as a continuous audit function (Bandyopadhyay *et al.*, 1999). Risk monitoring is an essential step in the overall management of risk and is required for good corporate governance.

Up to this point, risk and the management of risk have been discussed while only mentioning the influence of technology briefly. Even though risk, in general, may be

seen as a neutral concept, risks from an ICT perspective are definitely viewed as negative. The next section will introduce and discuss risks from an ICT perspective.

2.7 Risk Management from an ICT perspective

Information and communication technology (ICT) play a significant role in business. The benefits of using technology in business are numerous. Technology can be seen as a business enabler that helps to generate opportunities. However, as mentioned previously, in the pursuit of opportunities, risks are faced. Common risks in the information technology environment include natural disasters, data security risks, computer viruses, strategic risks as well as legal risks (Bandyopadhyay *et al.*, 1999). This section describes approaches used to manage ICT-related risks and will follow a similar outline at the general risk management discussions thus far in Chapter 2 as shown in Figure 2-1.

2.7.1 Risks from an ICT perspective

It was previously stated that risks can be perceived quite differently by different people in various situations and contexts. The same holds true for ICT risks. Blakley, McDermott and Geer (2001) define risk from an ICT perspective to be the possibility of an incident occurring which has a negative impact on the business. This suggests that risk from an ICT perspective is perceived negatively. "Risk is the **likelihood** of the occurrence of a vulnerability multiplied by the **value** of the information asset minus the percentage of risk mitigated by **current controls** plus the **uncertainty** of current knowledge of the vulnerability" (Whitman & Mattord, 2003), which is called the "risk identification estimate factor". ISO/IEC 13335-1 (2004)defines risk as "the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organisation". From this definition, three characteristics, namely threats, vulnerabilities and assets, can be distinguished.

An **asset** is anything that is useful or holds value for an enterprise. An asset can be tangible or intangible. A tangible asset's value can be accurately calculated. Examples of tangible assets include property and equipment (Fiksel, Low, &

Thomas, 2004). An intangible asset's value, on the other hand, is more difficult to measure precisely. Examples of intangible assets include reputation, brand equity, strategic relationships (Fiksel *et al.*, 2004) and information.

A **threat** is "a potential cause of an unwanted incident that may result in harm to a system or organisation" (ISO/IEC 13335-1, 2004). There are always threats present; some may be accidental, while others may be purposeful. There are five groups that threats are categorised into (Whitman, 2003). These are inadvertent acts, deliberate acts, acts of God, technical failures and management failures. Inadvertent acts are acts for which intent cannot be proven, such as deviations in quality of service providers (Whitman *et al.*, 2003). Deliberate acts are malicious and aim to inflict harm. These may include espionage, trespassing or theft (Whitman *et al.*, 2003). Threats outside of the control of humans are classified as acts of God, which include forces of nature such as storms, hurricanes and earthquakes (Whitman *et al.*, 2003). When machines or other equipment fail unexpectedly, these are classified as technical failures (Whitman *et al.*, 2003). Such failures include hardware or software failures. Finally, management failures are caused by management's inability to plan and anticipate changes in the enterprise (Whitman *et al.*, 2003).

A **vulnerability** is "a weakness of an asset or group of assets that can be exploited by one or more threats" (ISO/IEC 13335-1, 2004). Furthermore, such a vulnerability can be considered an avenue that a threat agent can exploit to inflict harm on an asset (Whitman *et al.*, 2003). Such a vulnerability can be accidentally triggered or intentionally exploited (NIST SP 800-30, 2001). Vulnerabilities could range from unlocked doors and computer networks without firewalls to a backdoor in a software application created by a programmer.

Assets, threats, vulnerabilities and other concepts are summarised in Figure 2-5 (ISO/IEC 13335-1, 2004). Various vulnerabilities (V) exist that may be exploited by threats (T) to cause harm to the assets. If a threat can successfully inflict harm

on an asset by exploiting a vulnerability, a risk (R) exists. Safeguards (S) may be applied to protect assets from threats. Residual risk (RR) exists where a safeguard had been applied but there is still a risk. All of these concepts must be considered to manage ICT-related risks effectively.

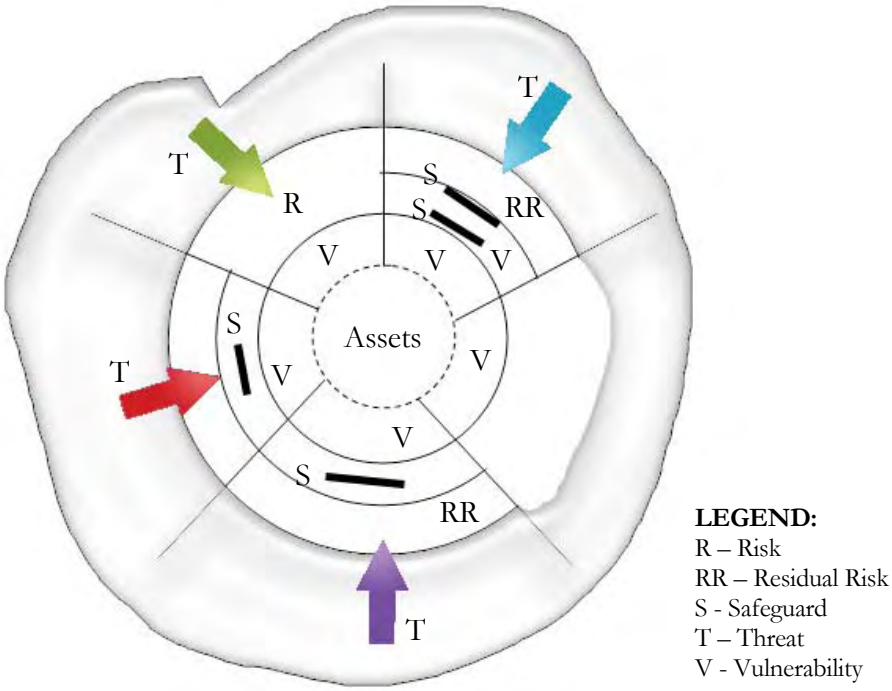


Figure 2-5: A Summary of ICT Risk-Related Concepts

2.7.2 Management of risk in ICT

Management of risk (Figure 2-3), from an ICT perspective, "is the process that allows IT managers to balance the operational and economic costs of protective measures and achieve gains in mission capability by protecting the IT systems and data that support their organisations' missions" (NIST SP 800-30, 2001). More detail, from an ICT perspective, on the management of risk will be offered in this section.

Approaches to risk analysis

Henry (2004) suggests three keys to risk analysis: namely knowledge, observation and business acumen. Knowledge about the environment wherein a business

operates, is needed, as well as about the various risks threatening the business. Observation, with the help of various tools available, enables information security managers to obtain a macro view of the environment in which the business operates. Furthermore, it is important for them to sift through it and draw the correct conclusions about the underlying scenarios, because of the vast amount of information available to information security managers. The last key is business acumen, where insight into the way the business operates is needed, and it is fundamental that the mission of the enterprise should also be considered.

After the keys, i.e., knowledge, observation and business acumen to risk analysis have been considered, and before risk analysis is performed, a risk analysis strategy should be chosen. Such a strategy should ensure that an approach is chosen that is suitable to the enterprise and that security efforts are focused to those areas where it is needed (ISO/IEC 13335-1, 2004). The approaches that can be followed include the baseline approach, the informal approach, the detailed approach or a combination of the three aforementioned approaches, also known as the combined approach (ISO/IEC 13335-1, 2004).

The baseline approach

With the baseline approach, the current safeguards of the organisation are identified and compared to industry peers (Ozier, 2004). Shortcomings are identified and protection is put into place (Ozier, 2004). It can be concluded that the baseline approach does not stop after risk analysis, but identifies controls as well, which can be considered to be part of risk management. All systems will employ the same baseline security with the baseline approach, regardless of the types of risk facing any given system (ISO/IEC TR 13335-3, 1998). This approach would be optimal if the security requirements of the organisation are relatively low, the organisation is small or all the systems are similar (ISO/IEC TR 13335-3, 1998).

Advantages of the baseline approach are that it only needs minimal resources to analyse the various risks (ISO/IEC TR 13335-3, 1998). The implementation process is greatly simplified, especially in large corporations, because several systems all make use of similar standards (ISO/IEC TR 13335-3, 1998).

Disadvantages would be that the level of security might be unnecessarily high if the baseline level is too high (ISO/IEC TR 13335-3, 1998). However, if the baseline level is too low, the exposure of the organisation could be too high (ISO/IEC TR 13335-3, 1998). Difficulties might arise regarding the management of the security, such as the upgrade of systems (ISO/IEC TR 13335-3, 1998).

The informal approach

The informal approach focuses more on practical results than on theories and principles. It makes use of noesis and experience of individuals to conduct the risk analysis.

The major advantage of the informal approach is that it is not resource intensive and requires little time and money (ISO/IEC TR 13335-3, 1998). There are, however, quite a few disadvantages. Firstly, there is the risk of something important being overlooked(ISO/IEC TR 13335-3, 1998). Secondly, it is difficult to justify the cost of the safeguards. Furthermore, people with limited previous experience in risk analysis might have difficulty analysing risks effectively (ISO/IEC TR 13335-3, 1998). This approach is also inclined to be vulnerability driven, i.e., controls are selected because a vulnerability exists without considering the existence of threats. Subjectivity is another disadvantage. The informal approach should be properly documented to ensure that findings are retained inside the organisation.

Based on the number of disadvantages that this approach demonstrates, it appears to be inadequate for most organisations.

The detailed approach

The detailed approach requires a comprehensive and in-depth risk analysis. It requires assets to be identified, threats and vulnerabilities to be assessed and safeguards to be selected. While the detailed approach covers all systems, and the results can be used to manage security changes, it is very resource intensive. It also requires a considerable degree of expertise. The detailed approach is discussed in more detail in the next section.

The combined approach

The combined approach is the approach used in most cases as it provides a balance. First, a high-level risk analysis is conducted. During the high-level risk analysis, all ICT-related risks are considered. For the crucial systems, a detailed risk analysis is performed (ISO/IEC TR 13335-3, 1998). For the other systems, a baseline approach is followed (ISO/IEC TR 13335-3, 1998).

2.7.3 Detailed risk analysis

Risk from an ICT perspective is viewed as the chance that a threat will exploit a vulnerability and cause harm to the organisation. This indicates that risk from an ICT perspective has three elements, which are threats, assets and vulnerabilities. The first three steps of a detailed risk analysis are, therefore, to identify each of these three characteristics (NIST SP 800-30, 2001). Figure 2-6 shows the risk identification activities for identifying ICT-related risks.

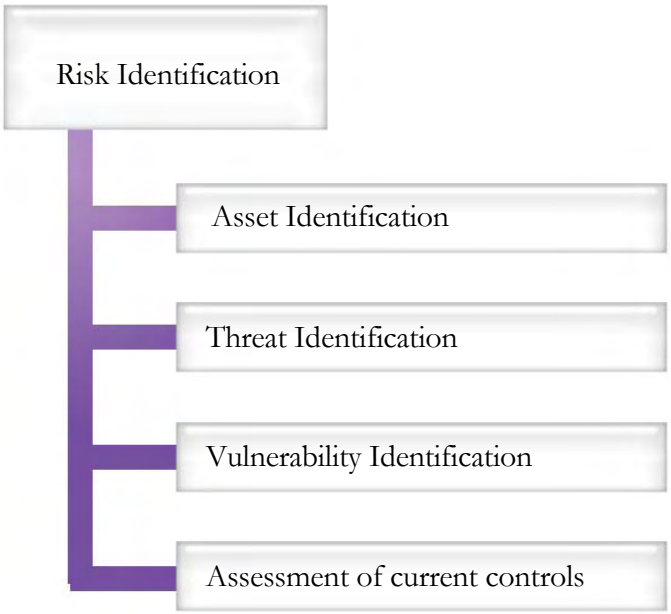


Figure 2-6: ICT Risk Identification Activities

Asset identification

The first step in the detailed risk analysis from an ICT perspective is system characterisation. During system characterisation, information regarding the various assets of the organisation is gathered. The first step identifies all the assets which are categorised according to the components of an information system, i.e., people, procedures, data, software and hardware (Whitman *et al.*, 2003). Thereafter, details about all of the identified assets are added, such as employee name, position, hardware serial number and manufacturer. When all assets have been identified, classified and the details captured, valuation of the assets is performed. Values are attached to the assets based on their value to the organisation. For ICT hardware or other physical assets which are easy to quantify, the replacement and maintenance values are used. The value of intangible assets, such as information, is more difficult to quantify. In this case, the value may be expressed as a security matter, for example, what it will cost the business in the case of loss of integrity, confidentiality or availability. Integrity, confidentiality and availability are known as the three pillars of information

security and are discussed in detail in Chapter 5. Quantitative valuation involves attaching monetary values to assets, while qualitative valuation involves attaching values of some descriptive nature to the assets.

After the basic valuation is completed, dependencies between the assets are identified. These dependencies between assets may influence their value. For example, if asset A cannot function without asset B, asset B is just as important as asset A.

The output is a list of all valuable organisational assets, the dependencies between the assets and a value assigned to each asset.

Threat identification

After the assets have been identified and valued, threats are identified. It is important that no threat be overlooked as this may cause serious harm to the ICT assets. Information regarding the various sources of threats to assets can be obtained from the users, owners or other personnel that work with or oversee the use of the assets (NIST SP 800-30, 2001). In addition, various outside organisations can be consulted to gain a better understanding of possible threats. These organisations can provide information such as threat statistics, thus, aiding the threat identification process (NIST SP 800-30, 2001). Care should be taken when considering information provided from outside organisations as it may be outdated, especially due to the rapidly changing ICT environment.

Examples of threats include acts of human failure, such as accidents and employee mistakes, and deliberate acts of information extortion, such as blackmailing employees for information disclosure.

After all threats have been identified, a list of these potential threats and the assets affected by them should be compiled (ISO/IEC TR 13335-3, 1998). In addition, the likelihood of the threats should be included (ISO/IEC TR 13335-3, 1998), which could be qualitative or quantitative.

Vulnerability identification

During vulnerability identification, weaknesses that a threat agent can exploit to inflict harm on an asset are identified (Whitman *et al.*, 2003). These weaknesses can be present in the physical environment, procedures, personnel, hardware, software, management, or communication software. Only vulnerabilities that are relevant to the organisation, based on their asset/threat associations, should be considered. However, vulnerabilities may arise when properties or attributes of an asset are used in a way unintended in its design. An example of such property is the small size of data storage components that are easy to transport. Such a small storage device can be easily concealed when stolen.

An important aspect to consider when identifying vulnerabilities of assets is the ease with which a vulnerability can be exploited. This should be considered for each asset-threat-vulnerability combination. For example, masquerading of user identities may be high due to the lack of user authentication, while the misuse of resources may be low, even without authentication, because the use of the asset has a low value to the user. It can be deduced that this process is cyclic in nature, because vulnerabilities should be considered when identifying threats.

Assessment of current controls

After assets, vulnerabilities and threats have been identified, the current controls that are in place, and those that are planned for implementation are analysed. The function of these controls is to minimise or eliminate the possibility of a threat exploiting a vulnerability, thus causing harm to an essential asset of the organisation. This identification of existing or planned safeguards is imperative to ensure that safeguards are not duplicated. Furthermore, it can be found that existing or planned safeguards are not necessary (ISO/IEC TR 13335-3, 1998). While current safeguards are identified, attention should also be paid to the condition thereof to ensure that they are working properly (ISO/IEC TR 13335-3, 1998).

Risk estimation

The outputs of the risk identification stage are considered when performing risk estimation. This assessment of risks is required to enable an organisation to select the most suitable controls to reduce risk. These characteristics of risk are used in risk estimation.

The first factor to consider, as mentioned previously, is the probability of a threat exploiting a vulnerability and causing harm to an asset, or rather, the probability of a risk (Frosdick, 1997). In the estimation, the outputs from the vulnerability and threat identification are used. Various databases exist that provide statistical data on the probabilities, such as those used in insurance and actuary institutions. Furthermore, intelligent guesses may also be made. This data is then analysed to determine the likelihood of a risk materialising.

The next factor to consider is the consequences of a risk on the organisation. These consequences refer to the value that the organisation loses due to harm that a threat causes when it exploits a vulnerability. Losses of value in tangible assets, such as hardware, are easy to determine. On the other hand, it is significantly more difficult to estimate the value of intangible assets, such as information and business processes, accurately. For example, if lightning strikes a power line and no surge protectors are in place, damage of computer hardware is certain (imminent). However, due to the hardware failure, some business processes cannot run for a period of time. This loss of business process is very difficult to quantify.

Risk evaluation

When values have been attached to the probability and consequences of the identified risks, these risks can be evaluated. Risk evaluation is the process of taking the values assigned during the risk estimation (Gerber & von Solms, 2005). The objective of risk evaluation is to prioritise risks and eventually to determine whether a risk should be accepted, avoided, mitigated or transferred.

The risk impact/probability matrix is a way to prioritise the identified risks, based on the probability of the risks, and the impact of the risk that has been identified during risk estimation. Such a risk matrix expresses the probability and impact (Conrow, 2003). Normally, a three-by-three matrix is used (Figure 2-4), while this may change depending on how granular an organisation requires risk evaluation to be. On a normal three-by-three matrix, the likelihood and impact is classified as high, medium or low. On different sized matrices, very high and very low may be added.

Once risks have been identified and estimated, these risks are plotted on the matrix. By plotting them on the matrix, a clear indication can be gained about how critical or severe they are. Identified risks are then listed in order of severity. This output from risk evaluation, and ultimately from risk analysis, is used in risk management to make decisions regarding the various risk control strategies.

This concludes the first part of the management of risk, namely risk analysis. Before risk management from an ICT perspective will be discussed, various additional aspects relating to risk analysis will be discussed.

The measurement of risk

While discussing risk management, qualitative and quantitative methods were mentioned. Quantitative risk analysis attempts to assign a precise value to the risk (AS/NZS 4360:1999, 1999). Annual Loss Expectancy (ALE), Livermore Risk Analysis Methodology (LRAM) and the Courtney Method are examples of quantitative risk analysis techniques. Intelligent guesses have to be made, because there is not always sufficient information available for risk estimation (Turn, 1986). This leads to some level of subjectivity in quantitative risk analysis. Qualitative risk analysis does not attempt to assign a monetary value, but uses descriptive scales such as high, medium or low (Schultz, 2004). Examples of qualitative risk analysis techniques include CCTA's (Central Computer and Telecommunication Agency) Risk Analysis and Management Methodology (CRAMM) and RISKPAC that both make use of fuzzy logic and questionnaires.

Qualitative risk analysis can also be regarded as subjective. This is because of a lack of good quality information (Blakley *et al.*, 2001). Quantitative and qualitative risk analysis techniques may also be combined to get the best results from the risk analysis process. Irrespective of the measurement technique used, the output of risk analysis will provide a prioritised list of risks that will be used to control various risks.

2.7.4 Risk Management in ICT

To reiterate some of the concepts discussed earlier, the management of risk consists of risk analysis and risk management (see Figure 2-3). When the first step, risk analysis that has been discussed in the previous section has been completed, attention is focused on the controlling and monitoring of risk. To control the various risks, one or more of the risk management strategies discussed earlier may be used. One technique that may be used to decide which strategy to be used is to look at the probability and impacts of the identified risks (see Figure 2-7). High impact, high probability risks, such as computer viruses, should be avoided (Conrow, 2003). High impact, low probability risks, such as fire, should be transferred (Conrow, 2003). Low impact, high probability risks, such as people misusing resources like bandwidth, should be mitigated (Conrow, 2003). Finally, low impact, low probability risks can be accepted (Conrow, 2003). However, where each risk falls depends on the risk appetite of the organisation and is decided on during risk analysis. This classification scheme, however, should serve purely as a guideline and the organisation should ultimately decide.

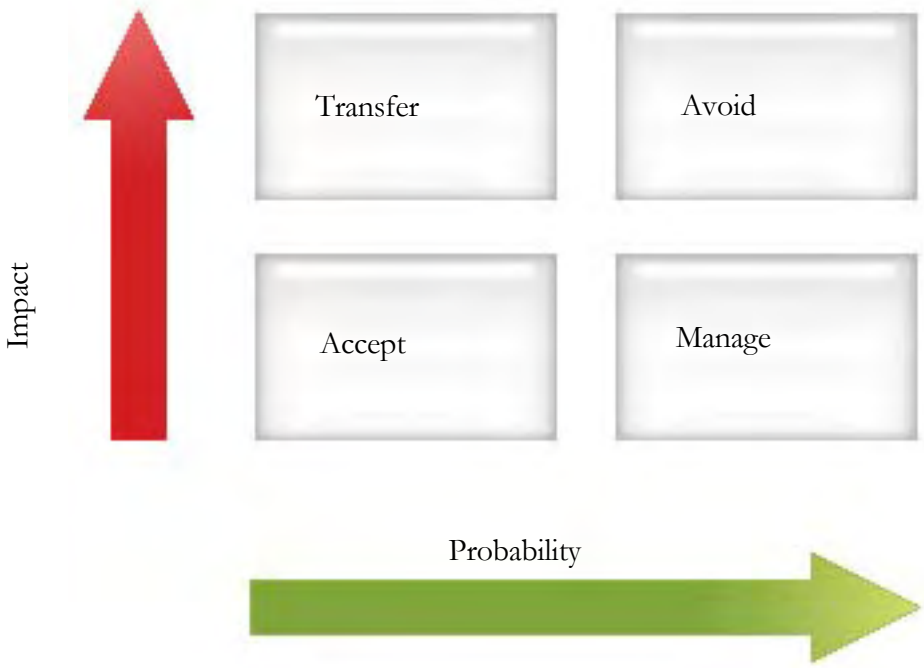


Figure 2-7: Risk Management Strategy Selection

Risk avoidance is a risk management strategy that seeks to prevent the exploitation of vulnerabilities. Whitman and Mattord (2003) state that this is the best approach as it is proactive and does not attempt to handle incidents after they have occurred. Whitman and Mattord also state that there are three general methods to avoid risks, namely application of policy, applying technology and implementing training and education. These methods avoid risk by countering threats, limiting access to assets and removing vulnerabilities in assets (Whitman *et al.*, 2003).

The goal of **risk transference** is to transfer risk to other assets, processes or organisations. An organisation can achieve this goal by reengineering business processes or outsourcing to other organisations that have better knowledge and experience regarding various types of risks (Whitman *et al.*, 2003). The key is for

the organisation to focus on their core business, and to let specialist consultants or firms handle the risks outside of their scope (Whitman *et al.*, 2003).

Risk mitigation attempts to minimise the impact of an exploited vulnerability by a threat. This is accomplished through careful planning and preparation. The key to risk mitigation is early detection of threats that exploit vulnerabilities. When an incident is detected too late, the impact may increase exponentially. Business continuity plans, incident response plans and disaster recovery plans all form part of this approach (Whitman *et al.*, 2003).

Finally, **risk acceptance** is the opposite of risk mitigation. Following this strategy an organisation would typically do nothing about risk and merely accept it (Whitman *et al.*, 2003). However, various questions should first be asked before any risks are accepted merely because they seem like the easiest choice to make. A flow diagram of these questions is shown in Figure 2-8 (NIST SP 800-30, 2001).

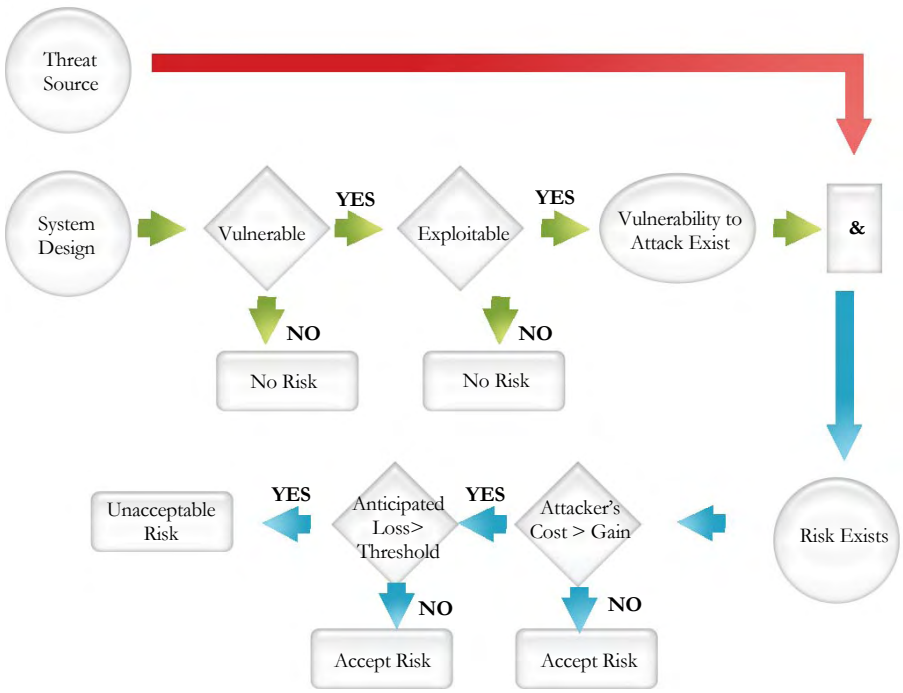


Figure 2-8: Risk Mitigation Questions

Controls to minimise risk

Controls are used to manage the risks once they have been analysed (Figure 2-3). Various controls exist that help to implement the above mentioned strategies. Tipton (2004) identified some of these controls and argues that they are all divided into three categories (Table 2-2). These categories are physical controls, technical controls, and administrative controls. Physical controls are tangible, such as locks, alarms and security guards. Technical controls are controls that consist of computer hardware, software or other related appliances and are also referred to as logical controls. Examples of technical controls include passwords, encryption and audit trails. Lastly, administrative controls dictate the behaviour of employees and processes (Hare, 2004). Examples of these include security policies and procedures, separation of duties and performance evaluations.

Tipton (2004) further breaks down physical, technical and administrative controls into preventative and detective controls. Preventative controls are proactive and aim to stop unwanted events from occurring before they do, while detective controls identify when certain events occur. A balance between preventative and detective controls is needed as preventive controls may limit users excessively, while too many detective controls might lead to an unrecoverable situation.

Additionally, controls can be classified as being deterrent, corrective or recovery oriented. Tipton (2004) argues that these are additional classifications to preventative and detective that are not specifically preventive or detective.

Table 2-2: Information Security Controls

PHYSICAL CONTROLS
Preventive
• Backup files and documentation
• Fences
• Security guards
• Badge Systems
• Locks and keys
• Backup power

- Biometric access controls
- Site selection
- Fire extinguishers

Detective

- Motion detectors
- Closed-circuit television monitoring
- Sensors and alarms

TECHNICAL CONTROLS

Preventive

- Access control software
- Antivirus software
- Library control systems
- Passwords
- Smart cards
- Encryption
- Dialup access and call-back systems

Detective

- Audit trails
- Intrusion-detection expert systems

ADMINISTRATIVE CONTROLS

Preventive

- Security awareness and technical training
- Separation of duties
- Procedures for recruiting and terminating employees
- Security policies and procedures
- Supervision
- Disaster recovery and contingency plans
- User registration for computer access

Detective

- Security reviews and audits
- Performance evaluations
- Required vacations
- Background investigations
- Rotation of duties

Table 2-2 above is represented graphically in Figure 2-9 below.

Table 2-2 above is represented graphically in Figure 2-9 below (GTAG 1, 2005). GTAG 1 also adds an extra dimension namely general controls and application controls.

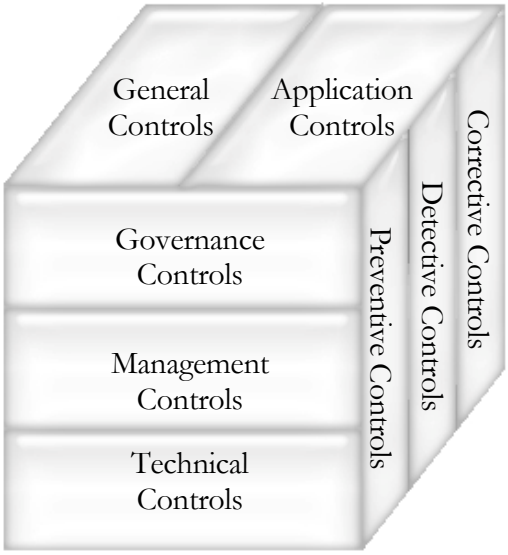


Figure 2-9: GTAG 1 - Classification

Risk monitoring

The last step in risk management is risk monitoring (Figure 2-3). Bandyopadhyay, Mykytyn and Mykytyn (1999) describe risk monitoring as an additional safeguard. The environment is continuously monitored for changes. These changes may include new threats materialising, or new assets that have been acquired by the organisation. The implemented controls are also monitored to ensure that they are still effective or necessary. Risk monitoring may also be used in auditing (Bandyopadhyay *et al.*, 1999). To assist with continuous monitoring, various computer assisted audit tools and techniques (CAATTs) exist (Bandyopadhyay *et al.*, 1999). Data analysis software is the most popular type of CAATTs. CAATT enables auditors to extract data from various file formats and databases and then perform common auditing tasks by making use of the functions built into the software. From this explanation, it can be clearly seen that auditing and risk management are closely related. By proactively monitoring and auditing risk, an enterprise will definitely ensure a competitive advantage and gain trust from various stakeholders.

2.8 Conclusion

Risk has been a universal concept that began when Eve convinced Adam to eat the apple. Since then, man has tried to predict uncertainty, or the unknown in his surroundings, from the tides by making use of the moon, to predicting rainy seasons by counting the days. Philosophers argue what risk exactly is, while risk, essentially, is merely a means to help describe the uncertain. Specialists in various fields have different interpretations; terms and definitions are used interchangeably. To manage this uncertainty, various means may be followed. This may include accepting that there are always uncertainties present, and that risk must be managed and turned into opportunities. Furthermore, the information and communications field are no exception to this. Despite the non-synchronous developments, ICT has kept up with other disciplines and has come up with numerous ways of conducting its own risk management. Because uncertainty cannot be taken out of business, it is very important for managers of businesses to ensure that risks are managed and opportunities are taken. Directors of public companies are also expected to practice risk management to ensure that shareholders' investments are protected. Risk management is only one of the issues to consider in corporate governance. Risk management and other corporate governance-related issues are discussed in the next chapter.

Chapter 3

CORPORATE GOVERNANCE

3.1 Introduction

The management of risk, discussed in the previous chapter, is a crucial element in any business. In this day and age, risk management cannot be mentioned without considering corporate governance, and vice versa. Most, if not all, of the corporate governance-related regulations take into account risk management. King II (2002) has a section dedicated to it as well as one on internal control. These two sections can be considered the twin components of the management of risk, as discussed in Chapter 2.

The objective of this chapter is to highlight the importance of corporate governance. In order to do this, it will follow this outline: what exactly corporate governance is, and why it is needed; its current guidelines and regulations; the duties of the various stakeholders, and finally, the relationship between it and risk management. Various examples of corporate governance failures will also be described.

3.2 What is Corporate Governance?

"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" (Cadbury, 1999).

While corporate governance has received a lot of attention recently due to scandals, such as Enron and Tyco, its origins can be traced back thousands of years, back to the separation of management and ownership of businesses (Wixley *et al.*, 2002). Owners needed to know that their business is managed effectively. The roles of auditors also came into existence from the separation of management and ownership and they check that the business is properly managed. The Industrial Revolution saw the commencement of multi-owner businesses. Due to the complexity of these multi-

owner businesses, certain legislation was needed to ensure that the interests of all the owners are protected.

Today, corporate governance can be described as "the system by which companies are directed and controlled" (King I, 1994) and encompasses (Naidoo, 2002):

- the development of and continuous monitoring of a system that ensures a proper balance of power exists inside a company;
- the development and implementation of a system that ensures that a company complies with all legal and regulatory obligations;
- the implementation of a process whereby risks are analysed and managed;
- ensuring that a process is in place that will keep the company accountable to the general society.

Thus, corporate governance is about thorough leadership, and this is the responsibility of the board of directors (King II, 2002). King defines these characteristics as:

- **Discipline:** the company and directors should be well behaved and follow generally accepted governance principles;
- **Transparency** ensures that an accurate view of organisational affairs can be obtained by stakeholders;
- **Independence** means the freedom from influences not concerning the well being of the company, while ensuring that decisions are objective and unbiased;
- **Accountability** should ensure that those who make decisions and act on them are liable to account;

- **Responsibility** refers to individuals that may be blamed if they are not performing within certain margins;

- **Fairness** allows all shareholders to be considered equally, notwithstanding their different positions and share count;

- **Social responsibility** concerns the elevation of social and ethical issues. Furthermore, the company must not discriminate or exploit any human or environmental source.

Tricker, the author of the first book on corporate governance (Garratt, 2003), argues that there are two key elements of governance, namely monitoring management performance and ensuring managers are accountable to stakeholders (Tricker, 1984). Tricker argues further that governance can be seen as a process that has four key activities: direction, executive action, supervision and accountability. Direction involves developing a long-term, strategic direction for the company, in other words, the vision of the company. Engagement in important top-level decisions is regarded as executive action. Supervision concerns the overseeing of how management is doing. Finally, accountability, similar to that discussed earlier, is ensuring that those that take action may be blamed for those actions.

3.3 Why Corporate Governance?

The major benefits of good corporate governance include the fact that well-governed companies attract more investment (Naidoo, 2002). Furthermore, investors are willing to pay a premium of up to 20 percent for companies that indicate they are well governed (Agrawal *et al.*, 1996). Well-governed companies also tend to implement sustainable growth better, (Naidoo, 2002) and have limited liability as they operate within set parameters. All this comes down to the fact that it makes good business sense to have a well-governed enterprise.

However, there are three common myths that hamper the improvement of corporate governance: that of the all-powerful chief executive; that a director's primary duty is to

the shareholders and that of executive and non-executive/independent directors (Garratt, 2003).

Numerous CEOs believe they own the company and that they may do with it what they want. This is not true, except in the case where the CEO is the major shareholder (Garratt, 2003). The myth that a director's primary duty is to the shareholders is not the case as when directors are appointed. They should focus on the demands of the company and not on the demands of the shareholders. In countries where case-law is used, all directors, i.e. executive and non-executive, should be regarded as equal.

There are also three "corporate sins", as mentioned by King II (2002): sloth, greed, and fear. Sloth occurs when flair is lost due to administrative dominance. Greed happens when directors make decisions that help themselves gain in the short term, while not considering the longer-term fortunes of a company, and fear is when directors become submissive to investors' demands. When this happens, the overall well-being and sustainability of the company may be at stake. Various guidelines on corporate governance have been developed to protect investors against mainly greed. In some cases directors may be so focused on preventing greed that they succumb to fear or sloth.

Ultimately, good corporate governance can be seen as a guarantee that investors will have a good return on their investments. If enterprises wish to gain trust and support from their investors and other stakeholders, they need to uphold the characteristics of good corporate governance, while avoiding corporate sins.

3.4 Learning from Other's Failures

This section highlights three examples of corporate failure and will be used in coming sections to clarify various issues of corporate governance.

3.4.1 Enron

The energy company, Enron, was founded in the mid-eighties and within 15 years grew to be the seventh largest company in the United States, employing over 21 000 staff in more than 40 different countries (Naidoo, 2002). In October 2001 a female employee accused Enron of corruption: the profits had been exaggerated, while millions of dollars of debt had been concealed, aided and abetted by some well-known US banks. Enron's employees were hard hit because their pension fund was, to a great extent, invested in what became worthless Enron shares. Various board members covered up their involvement and were found guilty of obstruction of justice. Enron filed for bankruptcy on the 1st December, 2001 (Wikipedia, 2006d). The extent of the Enron scandal underscores the importance of good corporate governance.

3.4.2 WorldCom

WorldCom, a US-listed telecommunications company, once channelled 50% of the world's Internet traffic (Naidoo, 2002). It supplied mission-critical communication services to numerous organisations worldwide, was the largest carrier of voice traffic in the world and owned 75 data centres on five different continents (Moberg & Romar, 2003). Additionally, it was worth over $190 billion (Naidoo, 2002). WorldCom approached financial reporting with an open-minded approach towards accounting rules (Moberg *et al.*, 2003). From January 2001 to March 2002, its profits were grossly inflated. Day-to-day expenses were accounted for as capital expenditure. By using this approach, WorldCom seemed much more profitable than it really was because these expenses were not reflected. In addition, personal loans to the value of $408 million were granted to various directors. WorldCom filed for bankruptcy protection in July 2002 after various disclosures on accounting irregularities, including violating GAAP, the generally accepted accounting principles (Moberg *et al.*, 2003).

3.4.3 LeisureNet

LeisureNet was the owner of the leading South-African health and fitness company, the Health and Racquet Club, which had 85 facilities country wide (Klein, 2001), with over a million members and 5400 full-time employees (Naidoo, 2002). In addition, it also owned 57.8% of HealthLand, a subsidiary which operated over 20 clubs in the UK, Europe and Australia (Klein, 2001). LeisureNet also owned various other leisure organisations, such as Imax and Planet Hollywood in Cape Town. The former joint chief executives, Gardener and Mitchell, also had an interest in the German firm, HealthLand (Naidoo, 2002). The acquisition of HealthLand by LeisureNet for DM10 million was fully supported by the board. Healthland was described as "a worthless shell". Gardener and Mitchell were paid by companies in which they were shareholders for "providing services". Effectively, Gardener and Mitchell were paying for personal belongings such as cars, boats, property and school fees with company money. Cape Town High Court judge, Hennie Nel said "..this illustrates the attitude of so many heads of companies who believe they will be allowed to walk scott-free from the financial disasters they have created", when he rejected applications to prevent disclosure of their international business interests. In essence, what the LeisureNet case comes down to is that the directors should not have hidden their interests in another company, not used the company for personal gain, and carried the interest of the shareholders and the company as a whole to heart.

3.5 Principles of Corporate Governance

The Asian Development Bank (ADB), together with Hermes Pension Management Limited, identified ten principles of good corporate governance. These attempt to differentiate between enterprises that put on a façade of good corporate governance, and enterprises that fully comply with the principles and spirit of good governance (ADB, 2003). There are three objectives of these principles. The first is to enable enterprises to develop and carry out their own corporate governance guidelines using

the principles as a benchmark. Next, to facilitate local and institutional investors that attempt to get the best of corporate governance in enterprises. Lastly to help governments in developing corporate governance regulations.

The ten principles are (ADB, 2003):

Performance orientation, i.e., increasing the enterprise's economic value. Using recognised metrics, such as ROE, ROI and EVA to make executive decisions that efficiently apply resources. This should be done for all shareholders and increases the enterprise's chances of increasing internal resources, as well as reaching environmental and social goals. These enterprises are also more likely to pay taxes and reward, cultivate and preserve human resources.

If an enterprise possesses a **nomination committee** with a formalised mandate and terms of reference, it is plausible that it may select the best possible directors available. Such a nomination committee should consist mainly of non-executive directors. In addition, a **compensation committee** ensures that the board's remuneration is adequate and market-related while ensuring that directors are retained and kept motivated (Naidoo, 2002).

Disclosure is about ensuring transparency, revealing true and accurate financial statements, material risks and explaining the logic behind all estimates (ADB, 2003). Furthermore, compliance with and deviation from corporate governance codes, goals, plans and development of the enterprise must also be made available. This should be done in a timely fashion so as to enable investors and other stakeholders to obtain a true reflection of the state of the enterprise's financial and governance aspects.

The principle of an **audit committee** is that it should concentrate on the key financial issues of the enterprise as well as managing a well-monitored system of internal controls (Naidoo, 2002). The committee should consist of mostly non-executive directors and be composed in such a way the a variety of knowledge and experience is available, such as accountancy, financial analysis and financial reporting (ADB, 2003).

"All enterprises must have a written **code of business conduct** and establish systems to ensure that it and all applicable laws are followed in the letter and spirit" (ADB, 2003). Shareholders want to know that enterprises do not support or enable, in any way, any form of misconduct, such as mismanagement, negligence of product or service quality, any form of bribery, and ignorance of the law.

The principle of **conflicts of interest** is important, too, because directors should act in accordance with the best interest of the enterprise, and they should ensure that all actual and potential conflicts of interest are disclosed. When there is a potential conflict of interest, that particular director should not be discussing them or make any decisions regarding them.

Environmental and social commitment. This is about ensuring that these needs are not neglected in the search for profits.

The **conduct of the board of directors** is the next principle. The board should be proactive, persistent and hardworking and should ensure that it is capable of what is required of it, while its conduct should set the tone for the whole organisation.

Responsibilities of investors means shareholders have a right and duty to monitor an enterprise's activities and partake in the voting process. In addition, the enterprise will profit from feedback provided from the shareholders. The board must ensure that minority shareholders are not mistreated.

The final principle is that of the **role of directors in turnaround situations** and concerns enterprises that are in trouble. In such a situation, the directors should be proactive, while averting discriminatory treatment of creditors. In addition, directors should not trade when the enterprise is insolvent.

3.6 Governance Regulations and Guidelines

The previous sections have established the importance of corporate governance. With this importance has come various published reports, which have guided boards on

how to effectively govern an enterprise. According to Vinten (2001), these reports started in the US during the late eighties, and their influence spread world wide. They include the Treadway Commission Report, the COSO Reports, and the Cadbury Report. Furthermore, a *combined code* has been consolidated from various best practices by various committees (Supportinet, 2006), and two of these inclusions into the combined code include the Cadbury and Turnbull Reports. The Treadway, Cadbury, Turnbull, King and SOX Reports will be discussed below.

3.6.1 The Treadway Commission Report

Various institutes and associations, including the American Accounting Association and the Institute of Internal Auditors, formed the National Commission on Fraudulent Financial Reporting, chaired by a former SEC commissioner, James Treadway Jr in 1985. The report of the Treadway Commission focused on the financial process and those who are involved in it, namely management, audit committees and internal and external auditors. The Treadway Report suggested 11 principles of corporate financial governance to enhance audit committee effectiveness. These were (Vinten, 2001):

- that ample resources and authority should be at their disposal to delegate responsibility;
- that the financial reporting process, as well as the internal control system, should be effectively, cautiously and cognisantly observed;
- that there be a review of the evaluation by management on the independence of the public accountants;
- that they oversee the quarterly and annual reporting processes;
- that the audit committee for all public companies should consist only of independent directors;

- that the audit committee should list their responsibilities and activities in the annual reports to the shareholders;

- that a charter for the audit committee should be articulated;

- that management plans regarding the advisory services by the independent public accountant should be reviewed before the commencement of each year;

- that if management chooses to seek second opinions regarding important accounting issues, the audit committee should be informed of these issues;

- that the audit committee, together with top management, should see to it that internal auditing is incorporated into the financial reporting process, and that it is fit and properly aligned with the independent public accountant; and

- that the programme established by management to ensure compliance with the code of ethics of the company should be annually reviewed.

"Most audit committee chairs see [these] recommendations as having exerted a positive influence on corporate reporting and internal controls", while the financial community is familiarising themselves with self-regulation (Vinten, 2001).

3.6.2 The Cadbury Report

The report of the committee on the financial aspects of corporate governance, also known as the Cadbury Report, was formulated by a committee chaired by Sir Adrian Cadbury and was preceded by the Treadway and COSO reports (Vinten, 2001). The report focused global attention on corporate governance (ITGI, 2003) and was considered the "world leader" (Vinten, 2001). The

Cadbury Report had a ripple effect that caused various best practices to be developed globally (Garratt, 2003). It is said that this report set the corporate governance "movement" into existence, particularly in Commonwealth countries. There were two driving factors behind the report, namely more accountability of board members and the prevention of corruption. While it was directed at companies listed on the London Stock Exchange (LSE), many non-listed companies also adopted the recommendations mentioned in it, which mainly addressed financial reporting and auditing while touching on more diverse aspects of governance as well. However, because financial reporting is very dependant on ICT, it cannot be separated and must be considered part of the financial reporting. To ensure standards of corporate behaviours are improved, transparency, integrity and accountability were recommended, while maintaining the fundamental character of an enterprise.

The report also identified responsibilities of the board regarding governance. Examples of such activities include setting strategic goals, offering sound leadership and monitoring management, as well as being accountable to stakeholders and providing a high standard of regular feedback to stakeholders. Ultimately, what the Cadbury Report achieved was the placing of power and accountability back into the hands of the board, while, at the same time, increasing its integrity towards its shareholders.

The Cadbury Report, in turn, gave birth to various other reports, called "the sons of Cadbury" by Vinten (Vinten, 2001). These included the Greenbury, Rutteman, Hample and Turnbull Reports. The Rutteman Report can be considered a watered down version of The Cadbury Report. Hample required the whole control system to be reviewed, not just the financial control system. Vinten argues that the Turnbull Report can be considered the most significant, as it focused on internal control and provides guidance for directors on the combined code and this will be discussed next.

3.6.3 The Turnbull Report

Also know as Internal Control: Guidance for Directors on the Combined Code, the Turnbull Report was formulated by a committee, chaired by Nigel Turnbull of the Institute of Chartered Accountants in England and Wales (ICAEW) and provides detailed guidance on how the "board should maintain a sound system of Internal Control to safeguard shareholders' investments and the company's assets" (Turnbull, 1999) forming the combined code. According to a KPMG Survey, before the report was published, very few UK companies had risk management and control processes in place.

This report focused on corporate governance in terms of risk management and internal controls and stated that risk management is ultimately the responsibility of a board, which must annually report on their risk management and other decision-making activities to their shareholders (Garratt, 2003). This discomforted various boards as they argued that risk management was the responsibility of management. In addition, the report required that the internal controls should be selected based on this risk analysis, and stated that all employees are responsible for internal controls. Again, Turnbull placed an emphasis on information and communication technologies.

3.6.4 The King Report on corporate governance for South Africa (King II)

The King Report on Corporate Governance for South Africa (King II) was inaugurated on 1 March 2002 and included a review of the King Code (King I) that was released in 1994 and which formalised governance standards applicable to companies listed on the Johannesburg Stock Exchange (JSE) and other large organisations (Naidoo, 2002). The report was named after the King Commission which was lead by Mervin King.

It focuses on the accountability and responsibility of management. According to Bornman (2004), various legislations have been published because of it (King I),

such as the Labour Relations Act (1995), the National Environmental Management Act (1997) and the Employment Equity Act (1998). The King II philosophy as Naidoo (2002) refers to it, is that the value system should be reflected in any context of governance. King II is based on an African value system that considers the collective good over the individual good and the spirit of humanity, also known as *ubuntu*.

The report was way ahead of its world counterparts at the time as it included the interests of a wider range of stakeholders beyond only financial aspects. It went beyond the conventional financial bottom line and introduced the triple bottom line, which included the financial aspects, but also social and environmental issues. In other words, the management of companies has to account for the profits, the people and the planet (Naidoo, 2002).

Risk management and internal control formed a significant part of the report, which emphasised that these are ultimately the responsibility of the board and are not limited to financial or strategic risks, but to operational ones, such as information technology.

3.6.5 The Sarbanes-Oxley Act (SOX)

The US Congress enacted the Sarbanes-Oxley Act (SOX) in 2002. The aim was to protect investors by ensuring that corporate disclosure and accuracy improved. Controls and reports relating to financial aspects received a lot of attention. and because ICT and financial aspects cannot be separated, information technology also played an important role. Other aspects also addressed, included author independence, corporate responsibility, better financial disclosure and conflicts of interest.

The act has 11 parts, called titles. Each title is divided into numerous sections. Two of these sections, 302 and 404 pertain particularly to information technology infrastructure. Section 302 is called *Corporate Responsibility for Financial*

Reports and describes the duties of a financial statement signing officer, including the revision of a financial report, ensuring the information presented is not misleading and fairly and accurately represents the financial situation in an organisation. Furthermore, the financial officer is also responsible for establishing and maintaining an internal control system, as well as communicating to various parties the effectiveness, efficiency of and changes to it.

Section 404, *Management Assessment of Internal Controls*, highlights that the annual report must contain an internal control report, which must state that management is responsible for the establishment and maintenance of such a system, as well as a means of financial reporting. In addition, the report must incorporate an assessment of the effectiveness of the internal control system.

The discussion above only highlights some of the guidelines and practices on the topic of governance. Other reports also exist, such as CoCo (1995) from Canada, and The Greenbury Report (Greenbury, 1995). Ultimately, these guidelines and practices attempt to protect the interests of investors who may not be actively involved in managing the company. The more recent publications also attempt to protect the environment and society at large by providing guidance to directors and other stakeholders in this regard.

3.7 Governance Roles and Responsibilities

Various corporate governance guidelines, such as those highlighted in the previous section, require that numerous tasks and duties be performed by respective stakeholders. While governance is concerned with what happens at the top, it may require more detailed tasks lower down the organisation's hierarchy. Some of these duties are highlighted below.

3.7.1 The board of directors

A board of directors is ultimately in control of an enterprise and responsible for the strategic direction of it. According to Encarta's Dictionary Tools (2005a), a board is "a group of people chosen to make executive or managerial decisions for an organisation". Its authority is derived from the articles of association (Naidoo, 2002). Furthermore, its composition, remuneration of and directions for the appointment of new board members are also traced from these articles (King II, 2002).

A board comprises executive and non-executive directors. Executive directors operate as managers of a company with day-to-day tasks and work full-time for salaries that are paid by the company (Encarta Reference Library, 2005a). In contrast, non-executive directors are not part of management and assist only on a part-time basis.

Directors are picked by management, usually for their personal, business or political contacts (van der Merwe, Appleton, Mahony, & Koen, 1995). According to The Hample Report (Hample, 1998) on Corporate Governance, a board must:

- carefully control the company while, at the same time, ensuring that it is advancing and taking entrepreneurial risks;
- have enough knowledge about the operation of the company to be accountable for its decisions, while keeping the strategic direction of the company in mind;
- consider profit-related aspects but take all stakeholders, i.e. employees, partners and general society, into account.

The most important responsibilities of a board comprise:

- setting the strategic direction;
- delegating authority;
- ensuring management is doing its work and implementing policies;
- ensuring an adequate system of internal control exists;
- being accountable;
- ensuring adequate communication takes place inside the company as well as with external stakeholders;
- finding a balance between the confines of governance and returning value to stakeholders (King II, 2002).

3.7.2 The chief executive officer (CEO)

The CEO, or managing director (MD), is usually a director of the company. According to Encarta Dictionary Tools (2005b), the CEO is "the highest ranking executive officer within a company or corporation, who has responsibility for overall management of its day-to-day affairs under the supervision of the board of directors". The CEO is appointed by the board and is involved in the day-to-day running of a company. Therefore, the roles of the CEO and the chair, which will be discussed next, should be separated (King II, 2002). This will ensure that a balance of power and authority exists at board level. The board should regularly review the performance of the CEO whose responsibilities include:

- developing a long-term strategy and vision for company and recommending that strategy to its board;

- developing annual business plans and budgets and recommending them to the board;
- attempting to ensure that the financial and operational goals and objectives are reached;
- seeing to it that the value and quality of the products and services offered are in a constant state of improvement;
- seeing to it that the company possesses an effective management team;
- articulating and supervising the execution of key corporate policies;
- being the main representative of the company.

3.7.3 The chairperson

"A chairperson is the presiding officer of a meeting, organisation, committee, or other deliberative body" (Wikipedia, 2006a). The chairperson of the board is responsible for it in contrast to the CEO who is running the company. For this reason it can be seen why it is recommended that the roles of chairperson and CEO should be separated. Commonly, the chairperson has the following core functions (King II, 2002):

- offering general leadership to the board;
- entering in activities relating to the selection of new board members, including their orientation and induction, as well an ensuring that they actively participate in company matters;
- articulating a formal work plan to ensure goals and objectives are reached, and participating in creating agendas for board meetings;

- being a key communication channel between the board and the management of the company;
- sustaining relationships between the company and its main stakeholders;
- ensuring that board members receive objective and accurate information that will enable them to make informed decisions.

3.7.4 Board committees

Various committees may be formed by a board to assist it, which indicates that it is capable of effectively delegating its obligations (Naidoo, 2002). A board committee performs a specific task. Furthermore, it can explore, in depth, issues that the board does not have time for. Some committees may be permanent, in which case they play a continuous role. Examples of permanent committees include audit and remuneration committees. Temporary committees play an *ad hoc* role, forming when needed and then disassembling when their tasks are completed.

When a committee is formed, the composition, objectives, purpose, activities, delegated authority, life span and reporting mechanisms to the board should be stipulated. Board committees should be allowed to accept outside advice when needed. Regular feedback should be given through the committee's chairperson to the board.

3.7.5 Shareholders

A shareholder is a person, company or other institution that holds shares of stock in a company. Ultimately, the shareholders own the company. By purchasing shares, they may share in the profits of the company (Wikipedia, 2006h). On the contrary, when the company does badly, the shareholders may lose money. Shareholders may have special privileges that depend on the type of

shares they own. Some of these special privileges include the right to vote, sharing of income as well as claiming assets when the company is liquidated.

In the past, corporate governance only protected shareholders. This is referred to as the shareholder concept. However, in recent times, corporate governance has expanded to include a wider range of people, called the stakeholders. Stakeholders are identified by the board and comprise the shareholders, and include society at large (King II, 2002).

3.7.6 Duties of directors

Garratt, one of the founders of the Commonwealth Association for Corporate Governance (CACG), offers ten directorial duties in his book, Thin on Top (Garratt, 2003). These duties are universally applicable. Each of these will be briefly discussed below.

The **duty of legitimacy** is the first of these and emphasises the importance to abide by national, as well as international, law. While this duty may seem trivial, it is of growing concern because the UK and US governments are moving cases of company law from civil to criminal courts, and directors may be held personably liable for corporate offences such as breaking fraud, health and safety, and pollution laws.

The next is **upholding the three values of corporate governance: accountability, openness and probity**. These have already been discussed in the section "What is corporate governance".

The **duty of trust** means directors abide by the law to ensure that the enterprise remains a going concern. Their decisions should reflect the long-term wellbeing of the enterprise and not their own short-term vision.

The **duty of upholding the primary loyalty of a director** means that a director should be primarily loyal to the company as a whole and not to those who appoint him or her.

The fifth is the **duty of care**. Directors should fully understand their roles and responsibilities and carry them out. Afterwards directors should be measured on how effectively and efficiently they performed the roles and responsibilities.

The **duty of critical review and independent thought** means each director on a board must be able to make their own judgement on the direction and internal controls systems to ensure a healthy enterprise. Therefore, each director must know their capabilities. Furthermore, directors should stay independent of each other and not beforehand agree to certain concepts and thereafter defend them as a group. At this point it is important to emphasise that each director has an equal vote on the board, and directors are compelled to use that vote. Directors may also raise any issue to be put on the agenda at meetings, which puts them in a very powerful position. In essence, due to the latest governance guidelines, the role of director is not as easy as it used to be.

In the **duty of delivering the primary roles and tasks of the board**, Garratt (2003) argues that the tasks of the directors may be described as four interconnected dilemmas:

- Ensuring the enterprise advances, while ensuring it is under sensible control;

- Ensuring there is enough knowledge of how the enterprise works, while developing a long-term, objective perspective of the happenings outside the business;

- Obtaining equilibrium between short-term, local requirements and national and international trends;

- Concentrating on the economic well-being of the enterprise, as well as keeping society at large in mind.

The **duty of protecting minority owners' interests** is self-evident: directors should not be the puppets of the major shareholders.

The **duty of corporate social responsibility** focuses on ensuring that society at large is considered. The social conditions of all stakeholders are improved, directly or indirectly, and companies realise that they are not anymore merely measured by financial successes: they should put something back into society as well.

The final duty is that of **learning, developing and communicating**. It is the duty of the board to learn from the decisions they make and the actions they take. Furthermore, the board must continuously enable the development of the various directors serving on the board. Lastly, it is of utmost importance that a channel for communication exists for all the stakeholders and that this is utilised extensively.

This section highlighted various tasks to be performed by the board, and the two important directors, namely the chairperson and the CEO. In addition, the role of board committees was discussed, and also underscored the importance of the shift from shareholders to stakeholders. Lastly, ten duties of directors were discussed. All the various roles and responsibilities also highlight the importance that a company should not be run by one person, the CEO, but a balance of responsibility is required.

3.8 Corporate Governance and Risk Management

Up to this point, various aspects of corporate governance have been examined. Amongst these aspects were the three corporate failures, numerous roles and responsibilities, as well as a chronological account of corporate governance reports on best practices. It can be ascertained that risk management plays a pivotal role in corporate governance, as it enables the perseverance of shareholder interests.

As mentioned earlier, the ultimate responsibility of a board is to offer strategic direction to an enterprise as a whole. In the search for a competitive advantage, a board must take certain entrepreneurial risks. As established in Chapter 2, there is a definite upside to risk - opportunity. A board should ensure that it is not guilty of the corporate sins of greed, sloth and fear. If it takes the right risks, a competitive advantage may be found. By performing diligent and proactive risk management, enterprises may become aware of issues that were not previously considered. Risk management empowers an enterprise to "gain a strategic discipline for operational excellence, as well as the power to create and influence its desired future" (Borland Software Corporation, 2005). The risk management of an enterprise is ultimately the responsibility of its board. It is also expected of a board to know what is required of it in this regard. King outlined various risk management duties of a board. These included the recommendation to make use of well-known risk management and internal control models and frameworks, to protect the assets and investments of the enterprise as well as supporting business objectives and sustainability. In addition, other issues surrounding risk management, such as uncertainty, opportunity and hazard, were also discussed. King II also clarified that risk management should be practiced throughout an enterprise and does not stop at board level, although risk management is ultimately the responsibility of the board.

3.9 Conclusion

This chapter highlighted the importance of corporate governance, as well as the relationship between it and risk management. Because risk is a measure to predict uncertain future events, and risk management attempts to manage these events, risk management is a crucial element of corporate governance. Indeed, by making use of risk management, investors may have much higher returns on their investments. Furthermore, a discussion on the various corporate guidelines and regulations has been offered to indicate the recent development of them worldwide.

While corporate governance recognises the value of risk management, various issues regarding it have become known in recent years. These include the "stovepipe"

approach to risk management that only considers risks in isolation. To solve these issues, enterprises worldwide are considering a new aspect, enterprise risk management, which will be discussed in the next chapter.

Chapter 4

ENTERPRISE RISK MANAGEMENT

4.1 Introduction

One of the major components of corporate governance, as was learnt in Chapter 3, is sound risk management principles. An example of this is King II (2002), which states that well-known risk management methodologies should be employed in addressing these organisational risks. One such type is enterprise risk management (ERM) of which there are various frameworks available. The objective of this chapter is to define and discuss ERM by providing a history of the stages of risk management that preceded it and explain its concepts and its frameworks. The negative aspects regarding ERM must also be discussed. The outline of this chapter will follow the above-mentioned objectives.

4.2 History of Enterprise Risk Management

Generally, the history of risk management evolved in three distinct stages: traditional risk management, business risk management and enterprise-wide risk management (DeLoach, 2000).

The first stage is only concerned with managing selected financial and hazardous vulnerabilities, generally managed by making use of financial instruments and internal controls. Additionally, one of the main features of traditional risk management is that risk is mainly perceived as being negative. DeLoach (2000) reports that the three principal defects of traditional risk management are:

- *Fragmented responsibility for risk management* – various departments each have a unique way of addressing risk management, thus numerous risks may go undetected.

- *The business risk portfolio is not considered* – focus is on individual risks, and this may lead to expensive risk response routines. Making use of a portfolio view of risk that indicates the relationships and similarities between risks across the whole enterprise, will help manage risk.

- *Risk management is not a product or a transaction* – and should not be seen as a commodity, but a strategic requirement, a business enabler that must be embedded in every aspect of business, from board level to the shop floor.

The next stage is **business** risk management, which moves away from being fragmented and narrowly focused to a more integrated, broader approach. DeLoach (2000) points out that a key force behind business risk management was the numerous non-financial incidents that affected enterprises negatively. Because of these, managers and boards are becoming more aware of the increasing number of risks not covered by traditional means. Top managers have realised that virtually all risks can be managed, and this has led to a more systematic approach to risk management. Managers were assigned areas of risk and were held accountable for them. Ultimately, business risk management is an improvement on traditional risk management, offering a formalised, structured approach to risk management.

However, this approach also has its downsides. The first is the fact that it only addresses risks, or groups of related risks. Next, it only addresses the negative aspects of risk: by only concentrating on these, exploitable opportunities may be lost.

The most current stage is **integrated risk management,** also known as enterprise, enterprise-wide or holistic risk management. Because the term may also refer to integration of only some risk management aspects, and ERM refers to all risk management aspects in an enterprise, this term will be used in the rest of this dissertation. While business risk management was a significant improvement on its traditional counterpart, it still has its limitations. ERM attempts to address these limitations and these will be discussed in the next section.

4.3 What is Enterprise Risk Management?

It was made clear in the previous section that ERM is the latest stage of the risk management evolution, which attempts to address the shortcomings of its predecessors. By no means does ERM attempt to create a risk-free environment, but empowers organisations to function more effectively (COSO ERM, 2004b). According to COSO, ERM is an enabler that aligns the enterprise risk appetite and strategy, links growth, return and risk, enhances risk-response decisions, minimises operational surprises and losses, identifies and manages cross-enterprise risks, and ensures that an integrated response is followed that addresses multiple risks, seizes opportunities and rationalises resources.

Two noteworthy definitions of ERM are by the Committee of Sponsoring Organisations of the Treadway Commission and the Canadian Treasury Board. The first defines it 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" (COSO ERM, 2004b).

The second expresses ERM as "a continuous, proactive and systematic process to understand, manage and communicate risk from an organisation-wide perspective. It is about making strategic decisions that contribute to the achievement of an organisation's overall corporate objectives" (Treasury Board of Canada, 2001). By comparing these two definitions, various overlapping aspects can be observed, such as that ERM is not a once-off endeavour, but a continuous process, that it encompasses all enterprise areas, and that it is a strategy linked to corporate objectives.

4.4 Components of ERM

Lam (2000) offers an outline of seven components which he calls "critical risk management issues that an organisation needs to consider." Each of these will be discussed in this section.

The first is **corporate governance**. Similar to that discussed in Chapter 3, Lam (2000) stresses that risk management is ultimately the responsibility of a board which has :

- to define the enterprise's risk appetite: the risk-to-capital leverage, the target department rating as well as the loss-tolerance of the enterprise;
- to ensure that adequate resources are in place that ensure risk is properly managed in order to sustain the business strategy;
- to incorporate risk management roles and responsibilities into the organisational structure, such as through a chief risk officer;
- to ensure credit, market and operational risks are managed by instigating a risk measurement and management framework;
- to implement a risk assessment and audit process while seeing that the enterprise keeps up with international best practices by employing a benchmarking strategy;
- to set an example for the rest of the employees to follow; and ultimately to sculpt a risk management culture throughout the enterprise;
- to act as catalyst that enables learning of new constructs throughout the enterprise as well as learning from experience.

The second issue to consider is **data and technology resources**, which should be utilised to assist with the management of enterprise risk. However, there are no off-the-shelf systems available that an organisation can buy to facilitate a complete solution (Lam, 2000). Therefore, enterprises are forced to either build their own solutions or buy various products and customise them. Lam suggests that the power of the Internet should be used when designing a custom system. One of the features of such a system should include the aggregation of portfolio data, which includes information captured in front and back office systems, and market data, which includes prices, volatilities and

correlations. Constant diligence should be applied to ensure that the data input is of a high quality.

The next issue to consider is **line management**. Because this is close to most of the origins of various risks, and because this is where it is easiest to quantify and assess them, it plays an important role. Line management is tasked with aligning business strategy to corporate risk policy by establishing risk acceptance criteria. This will help integrate risk management into new market and product opportunities.

Portfolio management should set targets and risk limits, ensuring appropriate diversification gets optimal returns. Risk portfolio management maximises shareholder value. **Risk transfer** goes together with portfolio management. Risk transference strategies should be employed after management has evaluated derivatives and insurances, as well as hybrid products that are available. Risk transference was discussed in more detail in Chapter 2. **Risk analysis**, a process that employs several risk metrics, has developed so much that market, credit and operational risks are constantly being quantified or qualified. These are also employed to choose the best risk-transference strategy. Various concepts surrounding risk analytics have been discussed in Chapter 2. **Stakeholder management** ensures transparency of the risk management processes. These enable possible investors to know what risk management practices are or are not followed and allows these investors to make decisions regarding investment in an enterprise.

4.5 Enterprise Risk Management Frameworks

Enterprise risk management is a paradigm shift in the manner in which enterprises manage their risks. Because ERM has to be applied throughout an enterprise in a top down, holistic manner, and because all organisations are different and have different resources and cultures, it is impossible to have a "cookbook" approach to it. Instead, a framework may be used, which can be considered a mould or template wherein various processes, methods or steps can be positioned. A discussion of three such frameworks is offered in order to obtain a general understanding of what is available and how these address the concept of enterprise risk management.

4.5.1 Treasury Board of Canada – Integrated risk management framework

This framework strives to support the decision making of public entities (Treasury Board of Canada, 2001). According to the president of the Canadian Treasury Board, Lucienne Robillard, "this framework will lead to the adoption of a more holistic approach to risk management and foster a working environment…".

This framework offers a way that allows organisations to analyse and discuss different risks, which may include any type "on the same page". Ultimately, its purpose is to (Treasury Board of Canada, 2001):

- "provide guidance to advance the use of a more corporate and systematic approach to risk management";
- "contribute to building a risk-smart workforce and environment that allows for innovation and responsible risk-taking while ensuring legitimate precautions are taken to protect the public interest, maintain public trust, and ensure due diligence"; and
- "propose a set of risk management practices that departments can adopt, or adapt, to their specific circumstances and mandate."

The Treasury Board of Canada's Integrated Risk Management Framework consists of four major elements that are summarised in Figure 4-1.

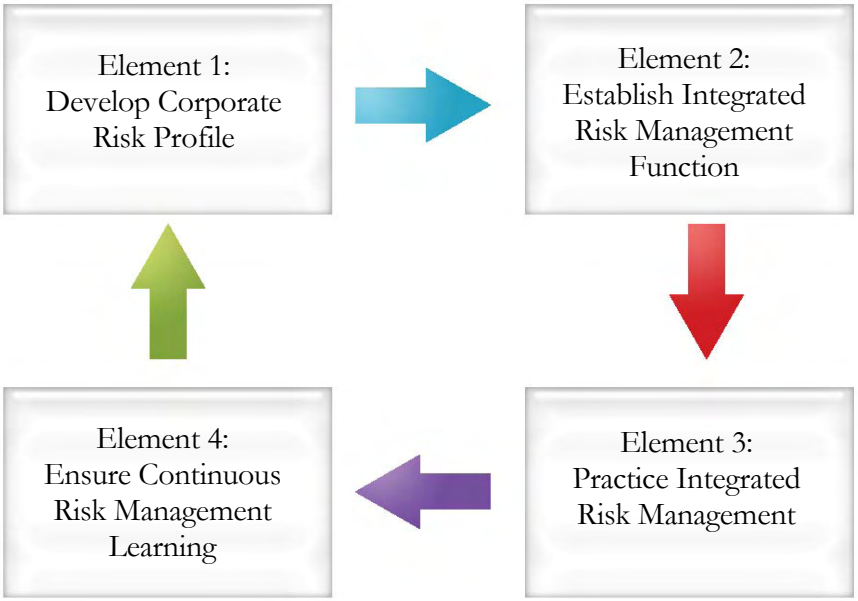


Figure 4-1: Treasury Board of Canada's Integrated Risk Management Framework

The first element is **developing the corporate risk profile** to examine threats and opportunities while also considering the objectives, available resources and corporate mandate. In order to do this an organisation must obtain a macro view of the operating environment by collecting information from all levels of the enterprise as to its current capacity to manage individual, group and whole enterprise as well as external risks. Scanning the environment, knowing the types and sources of and the impact and exposures to risk, the ability to control them is gained. It is also important to observe various trends over time that may act as an early warning system. A final aspect that must be taken into account is the risk appetite of various stakeholders. The following are the outcomes that are expected of the first element (Treasury Board of Canada, 2001):

- Opportunities and threats are identified by continuously monitoring the environment;

- The current situation regarding risk management within an organisation is analysed and includes the culture, current practices and challenges;

- The risk profile of an enterprise is established, including key areas and risk appetite.

Establishing an integrated risk management function involves preparing a corporate infrastructure that improves the understanding and communication of risk-related aspects internally. Such efforts offer clear direction and reveal the support offered by top management. The corporate risk profile offers input needed to establish the corporate risk management objectives and strategies which should be congruently aligned with the overall objectives and strategies of an enterprise, as well as the operating practices and organisational culture. This function must be integrated into the existing decision-making structures at the strategic and operational levels. In order to integrate risk management in a "rational, systematic and proactive manner", three outcomes should be sought (Treasury Board of Canada, 2001):

- Communicate, comprehend and implement risk management directives, such as vision, policies and operating principles;

- Implement an operational approach to integrate risk management while making use of existing decision-making structures;

- Foster the capacity to manage risk by making use of learning plans and tools.

Practising integrated risk management requires a definite management decision as well as a sustained commitment that will contribute to achievement of the organisational objectives by producing the following outputs (Treasury Board of Canada, 2001):

- A consistent process of risk management is applied to all levels of an enterprise;
- Risk management practices are integrated into informed decision-making and priority setting;
- Tools and methods that assist in decision-making are applied;
- Ongoing conferences with stakeholders take place.

Finally, **ensuring continuous risk management learning** is a fundamental issue so that more informed and proactive decisions are made, enabling more effective risk management and fortifying organisational capacity. The success of an enterprise depends largely on its state of readiness. The following outcomes are expected (Treasury Board of Canada, 2001):

- A supportive work environment is established where experience and knowledge is shared among peers;
- The integration of risk management practices into organisational learning plans;
- Risk management results are used to ensure that individual, group and organisational improvement is continuous;
- Best practices and experience are shared, internally and across government entities.

This framework does not explicitly address information or any of its supporting communication and technology aspects, but is still considered as a high-level framework. Moreover, it specifically addresses public services and focuses on the process and requirements of an ERM strategy. While this framework was

developed by a government agency, there are various commercial frameworks, such as the Grant Thornton enterprise-wide risk management framework.

4.5.2 Grant Thornton enterprise-wide risk management framework

This framework is based on a general risk management cycle, summarised in Figure 4-2. Because it is very similar to the issues raised in Chapter 2, it will not be discussed again. The resultant risk profile of the first three steps is summarised in Figure 4-3. This framework allows for centralised and decentralised risk management models. In addition, legislation, such as the Sarbanes-Oxley Act, is also acknowledged. Six elements must be in place before the framework is developed (Booker, 2003):

- Support from senior management;
- Proactive, rather than static, efforts;
- Clarity and understanding of the various risks;
- Individual accountability;
- Suitable resources;
- A culture to enable risk management.

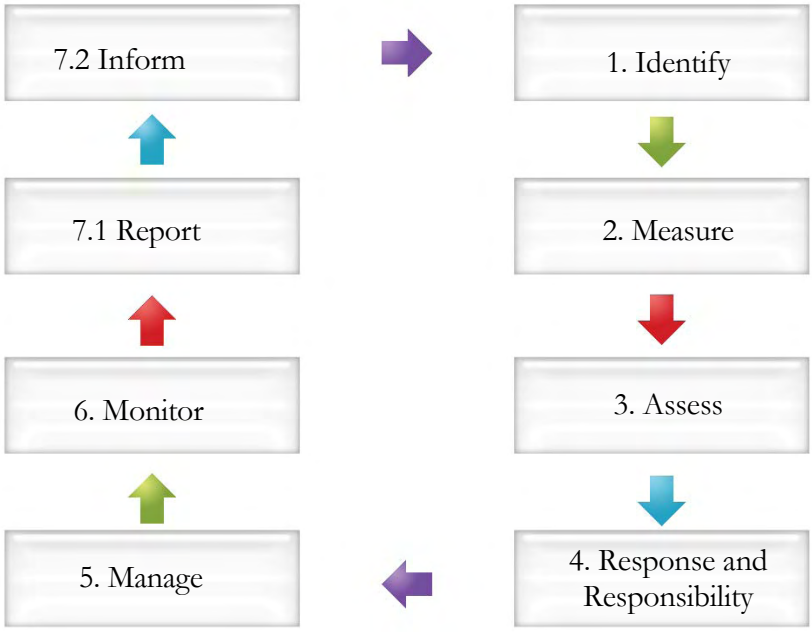


Figure 4-2: Grant Thornton ERM Framework

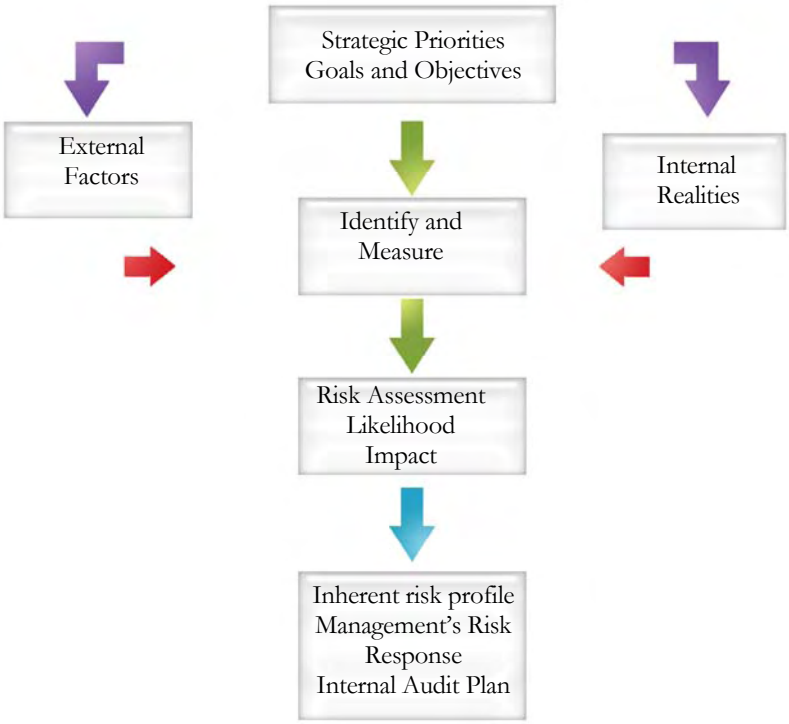


Figure 4-3: Grant Thornton ERM Risk Profile

4.5.3 COSO ERM framework

The Commission of Sponsoring Organisations (COSO) of the Treadway Commission was formed in the early nineties to address internal control shortcomings. The commission consists of members of the financial community and published an Integrated Control – Integrated Framework in 1992. After this framework was published, internal control was seen as a process rather than "just a list of objectives and controls" (Leitch, 2005). This framework became the *de facto* standard to address internal controls that are widely used by the accounting industry. The COSO ERM Framework was published in 2004 and "shows great knowledge of risk management and techniques and contains many interesting examples" (Leitch, 2005). The objectives of the framework are to (COSO ERM, 2004a):

- Produce a conceptually sound framework that offers common terminology, integrated principles and practical implementation guidance;

- Be the common foundation between various parties to learn and communicate about ERM and its benefits and limitations.

This framework comprises the three dimensions depicted as a plane on X-Y-Z axils which are illustrated as a cube in Figure 4-4. The first plane (front view) represents the eight components, according to COSO, that comprises ERM, and is similar to the components discussed earlier. The second plane (top view) represents ERM objectives while the third plane (side view) represents its business levels.

ERM consists of eight interrelated components, deduced from how a business is managed, and represented in the front view of the framework. The first component, **Internal Environment**, concerns the people of the organisation who drive the business, and the environment wherein they operate. They

influence the risk philosophy and appetite of an organisation. After these have been established, objectives must be set to reflect the mission, vision and risk appetite of the entity. This is called the **Objective Setting**. The next component is **Event Identification,** where the internal and external events that may influence the implementation of strategy and achievement of goals are identified. These include both the upside, opportunities, and the downside, risks. In order to scrutinise interrelationships between risks across the enterprise, a portfolio view of them is taken. After a risk portfolio has been developed, it is analysed by **Risk Assessment** in order to determine how risks should be managed. **Risk Response** activities follow as management decides on an approach to follow. These response activities are the same as those discussed in Chapter 2, namely avoidance, acceptance, mitigation and transference. **Control Activities** that follow include policies and procedures that are established and carried out that ensure that the selected responses are performed effectively. **Information and communication** concerns the capture, processing and communication of relevant information in a timely manner that will ensure that personnel can fulfil their risk management duties. Finally, **Monitoring** pertains to the observation of the ERM process that enables the process to be dynamic and the enterprise to offer quick responses. This may be exercised as ongoing management activities and/or separate ERM evaluations.

The second plane (top view) of the framework stipulates the objectives of the enterprise, although distinct, may overlap. The first are the high-level **Strategic** objectives, which support the mission, vision and goals of the enterprise. Lower-level objectives, such as **Operational** ones relate to the effective as well as efficient use of organisation resources. Public-trading enterprises have to adhere to various **Reporting** objectives, specified by various government regulations. Considering the current nature of reporting, IT will play a significant role. Finally, the **Compliance** objective refers to how carefully the enterprise abides to current legislation. A level of overlap can be observed between compliance by legislation relating to reporting.

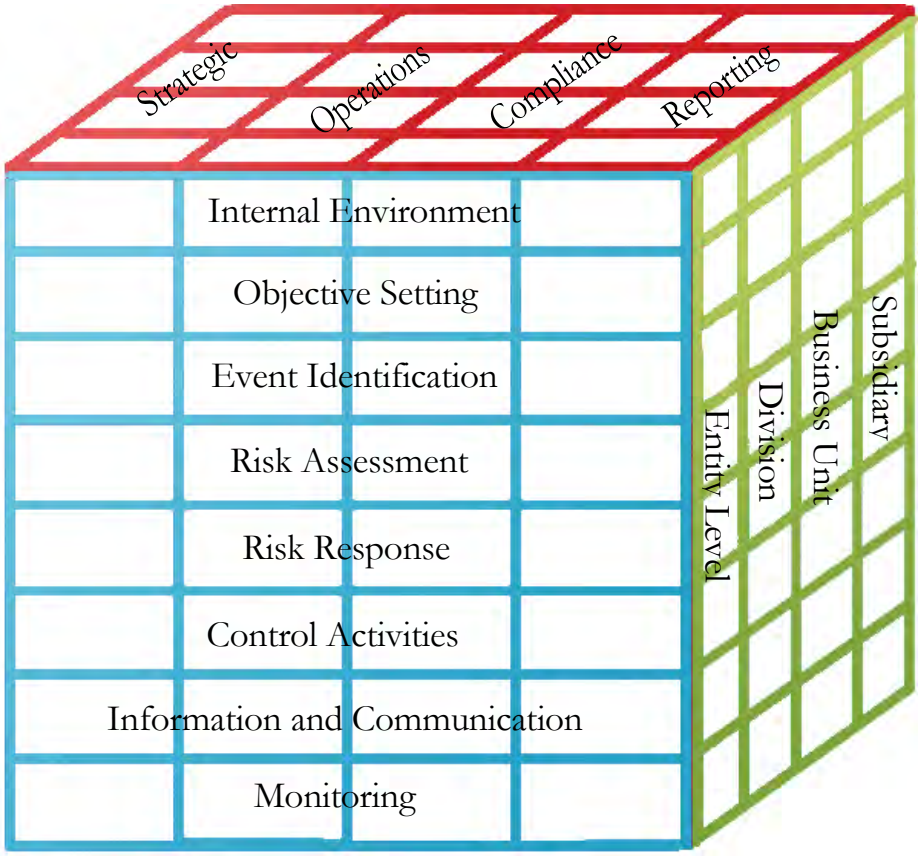


Figure 4-4: The COSO ERM Framework

The third plane considers ERM at four organisational levels, namely **subsidiary**, **business unit**, **divisional** and **entity** levels. ERM can be considered for every cell in the cube-shaped framework. For example, one can consider the front, top left cell that represents the internal environment's strategic objectives for a specific entity in the enterprise.

Bornman (2004) argues that this framework can be applied cyclically, similar to the Grant Thornton and Canadian Treasury Board ones although it is not specified. While there are various frameworks that assist in ERM, there are still various issues to be addressed that can be considered "roadblocks" to the wider acceptance of ERM. These will be discussed in the next section.

4.6 Limitations to ERM

ERM, according to the COSO definition, only provides reasonable assurance as to the achievement of objectives by management and a board (COSO ERM, 2004b). Absolute assurance, however, is very difficult to achieve because risk pertains to the future which no one can predict with certainty. Moreover, there are always events that fall outside the control of management, while in reality, no business process will always function as expected. In effect, even perfectly applied ERM may have trouble from time to time.

The COSO report discusses five limitations to ERM, which are:

- *Judgement* – ultimately, all business decisions are made by humans who have to apply judgement based on available information in limited time, under variable business conditions. The effectiveness of ERM is limited by these judgements.

- *Breakdowns* – this may be caused by misunderstandings, inexperience, judgement mistakes, carelessness, distractions or fatigue.

- *Collusion* – this is caused by people conspiring to commit and hide activities to meet targets or to gain financially from them.

- *Costs versus Benefits* – resource constraints must be considered by weighing the possible benefits, the cost failure and the resources required.

- *Management Override* – while the process design may be flawless, management can override ERM processes for reasons such as hiding the lack of compliance or meeting targets.

Another limitation to the ERM frameworks discussed in this section is the lack of "linkage" to other industry standards: there are just too many of them. It can be argued that this linkage should be supplied by other industries, rather than by COSO itself.

4.7 Conclusion

ERM, while still a relatively new concept, has been accepted by the international business community with open arms. Companies like Microsoft and the Unocal Corporation have adopted ERM with reasonable success (Barton, Shenkir, & Walker, 2002). As more and more companies adopt this concept, more will benefit from the lessons learnt. As various stakeholders participate in the development of such frameworks, a knowledge-based solution may be created. However, ERM is not without its flaws, such as the lack of information-related concepts and how it must be managed.

ERM has been discussed because it will play an important role in the later chapters as it will be used as a side of a proposed model, EPiRISMM. Before the model will be discussed however, information security and problems regarding it will be highlighted in the next chapter.

Section 3: Problem

Chapter 5

ICT RISK MANAGEMENT: THE PROBLEM

5.1 Introduction

Corporate governance is ultimately concerned with the strategic management of an enterprise. The board, amongst others, is responsible for overseeing the risk management and may be held accountable should anything go wrong. Indeed, should something go wrong with an enterprise's important information systems, board members may face a jail sentence. Due to the different outlooks on risk management of ICT and the enterprise, being a board member can be a daunting task. This chapter emphasises the incoherence between the ICT and enterprise environments and will first describe why information is so important, where after general information security concepts will be discussed. An explanation will follow on how information and the supporting technology have become so important to enterprises. An analogy will be used to compare risk management vantage points. Finally, the problem regarding the discontinuity will be discussed.

5.2 Why Information is Important

"Information as a concept bears on a diversity of meanings, from everyday usage to technical settings. Generally speaking, the concept of information is closely related to notions of constraints, communication, control, data, form, instruction, knowledge, meaning, mental stimulus, pattern, perception, and representation" (Wikipedia, 2006e). While the concept of information may be interpreted in various ways, it is also considered a valuable asset to most enterprises today. In fact, it is considered that "information has become the key resource and even the life blood of many organisations" (Halliday *et al.*, 1996). Furthermore, information is considered the "glue that holds an organisation together and allows all other resources to be managed" (Eloff, Labuschagne, & Badenhorst, 1993). Information is considered pivotal in the way that enterprises execute their day-to-day operations and may also be considered

the "glue" in the supply chain. Technology has been designed to help organisations utilise their information more effectively and efficiently. Information and the supporting information and communications technology cannot be considered separately these days. Indeed, "[i]nformation technology is reshaping the basics of business. Customer service, operations, product and marketing strategies, and distribution are heavily, or sometimes even entirely, dependent on IT. Information technology, and its expense, have become an everyday part of business life" (Keen, 1991).

Although information and ICT cannot be considered separate these days, this dissertation will distinguish between the two, because information can be considered to span much wider than just ICT, which would include verbal communication and information on paper.

Information, in general, is critical for two aspects: learning and decision-making (Heeks & Duncombe, 2001). Therefore, it is important that the right information is available at the right time and in the right place, which will enable various stakeholders to learn from the information offered and make informed decisions.

5.3 What is Information Security?

To ensure that confidential and accurate information is available when it is needed, an organisation must ensure that its information is secure. "Information security deals with several 'trust' aspects of information…[i]nformation security is not confined to computer systems, nor to information in an electronic or machine-readable form. It applies to all aspects of safeguarding or protecting information or data, in whatever form" (Wikipedia, 2006f). Information security, from an information system point of view is defined as "the protection of information systems against unauthorised access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorised users or the provision of service to unauthorised users, including those measures necessary to detect, document, and counter such threats" (CNSS, 2006).

There are various misconceptions regarding information security. One of these misconceptions is that computer security, IT security, ICT security and network security are the same. These terms are often used interchangeably. Moreover, there are some misconceptions regarding information security and information risk management. Some, including Blakley, McDermott and Geer (2001), argue that information security is information risk management. Others argue that information risk management is a subset of information security.

Information security, in general, consists of three widely accepted pillars, or elements, which are based on three characteristics of information. These are confidentiality, integrity and availability, and are commonly referred to as the CIA triad. The CIA triad is based on the term "the right information to the right users at the right time". The first pillar, **confidentiality**, is defined as "the quality or state of preventing disclosure or exposure to unauthorised individuals or systems. Confidentiality of information is ensuring that only those with rights and privileges to access a particular set of information are able to do so, and that those who are not authorised are prevented from obtaining access. When unauthorised individuals or systems can view information, confidentiality is breached" (Whitman *et al.*, 2003). In other words, confidentiality is the offering of information *to the right users*. **Integrity**, the second pillar, is defined as "the quality or state of being whole, complete, and uncorrupted". In general, information integrity can be compromised accidentally, such as hard-drive crashes or errors in transmission, or maliciously, such as packet interception and alteration (Wikipedia, 2006c). In other words, integrity refers to *the right information*. Whitman and Mattord describe **availability**, the final pillar, as enabling "users who need to access information to do so without interference or obstruction, and to receive it in the required format" (Whitman *et al.*, 2003). Availability of information is compromised during power outages or hardware failures. Thus, availability refers to the information that is provided at the *right time*.

However, while the abovementioned pillars were adequate in the days of the mainframe computers, they are not sufficient any more. To keep up with the changing

environment, various other characteristics of information that pertain to information security have been added to the CIA-list. These are accuracy, authenticity, utility and possession. **Accuracy** refers to information that is error-free and offers the value that the user expects (Whitman *et al.*, 2003). Next, **authenticity** refers to information that is "genuine and original, rather than a reproduction or fabrication". **Utility**, on the other hand, is information that has value for a purpose or user. Finally, **possession** indicates ownership or control of information.

In addition to these seven qualities, there are others, such as non-repudiation, accountability, auditability and privacy (InfoSecPedia, 2006). Furthermore, authorisation and authentication may also be added, but experts agree that these are mechanisms rather than goals (InfoSecPedia, 2006).

By exploring the qualities of information, it becomes obvious that information has become a valuable commodity. Business users cannot work without quality information anymore. With information's value increasing exponentially across most business sectors, its protection has become a matter of concern, both nationally and internationally. In order to protect these assets, good standards and practices for their protection have been formulated and are used, in many cases, globally, to prevent the misuse of information and to keep it secure. Some of the key security guidelines and regulations will be discussed next.

5.4 Information Security Guidelines and Regulations

In the previous section, the importance of information has been reinforced and various characteristics pertaining to the quality of information has been discussed. In order to guard against information-related risks, various guidelines, regulations and standards have been developed over the years. Five of these, namely NIST, CobiT, the 17799 family, ITIL and the GMITS family will be discussed next.

5.4.1 NIST SP 800-30

The National Institute for Standards and Technology's (NIST) special publication's purpose is to provide "a foundation for the development of an effective risk management program, containing both the definitions and the practical guidance necessary for assessing and mitigating risks identified within IT systems. The ultimate goal is to help organisations to better manage IT-related mission risks" (NIST SP 800-30, 2001). NIST SP 800-30 describes the process of risk assessment of Information and related assets, such as described in Section 2.6.3.

5.4.2 BS 7799 family

The BS 7799 family as described here, consists of ISO/IEC 17799 (2005), which has descended from BS 7799 part 1, and ISO/IEC 27001 (2005) , which has descended from BS 7799 part 2. In 2000, BS 7799 was formally accepted as an international standard. ISO/IEC 17799 "sets out guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organisation. It contains best practices regarding control objectives and controls in information security management" (ISO/IEC 17799, 2005). The 2005 version of ISO/IEC 17799 consists of 12 main sections, outlined below:

- Risk assessment and treatment;
- Security policy;
- Organisation of information security;
- Asset management;
- Human resources security;

- Physical and environmental security;
- Communications and operations management;
- Access control;
- Information systems acquisition, development and maintenance;
- Information security incident management;
- Business continuity management; and
- Compliance.

ISO/IEC 27001 (2005) describes how to implement ISO/IEC 17799 and how to establish an ISMS, an Information Security Management System (Whitman *et al.*, 2003). The methodology for this implementation can be described in four high-level steps, namely plan, do, check and act. The detailed steps for this methodology will be revisited in Section 7-3 as they will be used in the model represented later on.

5.4.3 ITIL

The focus of ITIL (Information Technology Infrastructure Library) is to align IT infrastructure with the organisation's needs. ITIL strives for high quality IT services through a best practices framework (Wikipedia, 2006g). Fundamentally, the ITIL framework consists of management procedures that enable the business to attain high quality IT procedures as well as value for money.

ITIL was developed during the 1980s and is today still maintained by the Office of Government Commerce (OGC), which is a part of the treasury in the UK. ITIL, as the name suggests, is a library, a collection of books, each of which address an aspect of IT management. These aspects include the following:

- Incident management;
- Change management;
- Problem management;
- Service-level-management;
- Continuity management;
- Configuration management;
- Release management;
- Capacity management;
- Financial management; and
- Help desk management.

While ITIL mainly focuses on ICT service management, there are various components of information security inherent in it. Some of ITIL's information security focuses include availability management, IT service continuity management, pro-active problem management and incident management. An example of an approach to ICT security is CobiT (Control Objectives for Information Technology), which focuses on implementing controls to protect ICT assets against risk.

5.4.4 CobiT

CobiT was authored by ISACA (Information Systems Audit and Control Association). The CobiT product family consists of six publications, namely the executive summary, the framework, control objectives, audit guidelines, implementation tool set and management guidelines (Wikipedia, 2006b).

The CobiT framework indicates how the business can reach its objectives in the IT processes. In addition, 34 high-level objectives are described over four domains, namely planning and organisation, acquisition and implementation, delivery and support, and monitoring (IT Governance Institute, 2000). The CobiT control objectives describe 215 detailed control objectives within the 34 IT processes and four domains. The CobiT audit guidelines recommends activities that must be performed that enables consistent and continuous auditing of IT procedures. Next, the CobiT implementation tool set contains management awareness and IT control diagnostics, an implementation guide, frequently asked questions, case studies, and slide shows. The latest implementation toolset also contains lessons learnt from companies that successfully implemented the previous versions of CobiT. Finally, the management guidelines consist of maturity models, critical success factors, and Key Performance Indicators (KPIs). These will ensure that any concerns of the stakeholders of the enterprise are eased.

5.4.5 GMITS family

GMITS (Guidelines to the Management of Information Technology Security) is a joint effort of the International Organisation for Standardisation (ISO) and the International Electro-technical Commission (IEC). GMITS is divided into five parts published as ISO/IEC Technical Report (TR) 13335-1 to 13335-5. The first two parts of GMITS are not published as a technical report anymore, but is combined into what is now known as ISO/IEC 13335-1.

ISO/IEC 13335-1 is directed towards managers that are involved in overall security management and those involved in ICT security management. High-level definitions, concepts and models are provided to give top management a briefing on ICT security that will enable them to make informed decisions on the subject.

The old part 2 of GMITS (ISO/IEC 13335-2) is aimed at lower levels of management than that of part 1 and delineates ICT security-related aspects aimed at this level of management. Part 2 emphasises the importance of an ICT security plan and describes how the ICT security endeavour forms part of the organisation. Part 2 also describes possible risk management strategies, such as those described in Section 2.6. In GMITS part 3, the implementation of the security aspects described in part 1 and 2 are covered and security techniques are described such as the execution of a detailed risk analysis (See Section 2.6.3). These first three parts of GMITS will be used in the later stages of this dissertation. However, there are two more parts of GMITS. They are GMITS part 4 which describes the selection the selection of safeguards and GMITS part 5, which describes the management of network security.

This section described four standards and best practices used to manage information and related risks. Some of these standards and best practices will be used later on in the proposed model, EPiRISMM, where a distinction will be made between those that focus more on information and those that focus more on the ICT infrastructure. The next section will inquire into how businesses became so dependent on information and its supporting technology.

5.5 The Evolving Dependency on Information

"About 20 years ago, no one had heard of a CIO (Chief Information Officer) and only a handful of organisations were using the phrase 'information technology'" (Hwang, 2002). Back then, it was the job of the information resources manager to determine which room-sized computer to buy (Hwang, 2002). These room-sized computers were running batch applications that were instructed using punch cards. Today, a vast number of computers are connected to the information super-highway and are driven by the multitasking distributed computer arena. Over the years, the "computer environment changed from a computer-centric environment to an information technology-centric environment" to an information-centric environment (Gerber &

von Solms, 2001). This section will discuss the evolution of dependency on information.

Up to the 1980s, a business's computer department was seen as a separate department, though considered important. Very little, if any, organisational departments depended directly in real time on the computer department. Computer downtime did not have a significant impact on the other departments. This is indicated in Figure 5-1(a). As multitasking, distributed processing and real-time control became more popular, companies realised the benefits of a better relationship with the, now called, information technology department (Moses, 1992). As can be seen in Figure 5-1(b), the various organisational departments are now more dependent on the information technology department. In the case of an information technology department's failure or disruption, the other departments will also face a degree of disruption, and the business could be adversely affected. In the information-centric era, or the information age, which started in the early nineties, an IT department was more integrated in the business than ever. The flow of information through an organisation is as important as the flow of blood through the human body; and experts have stated that "having the right information at the right time could make the difference between profit and loss, success and failure in today's business environment" (IWS, 2005). This dependence on information is depicted in Figure 5-1(c). It is even possible to take it further today, by admitting that not only are there intra- and extra-organisational bonds, and that not merely all departments, but various organisations are so integrated and entangled, that it is impossible to try to separate them, with information being the glue that keeps them together. Organisational barriers, thus, are becoming blurred. This is depicted in Figure 5-1 (d), where communication is happening up and down the supply chain, and the Internet is pregnant with opportunities.

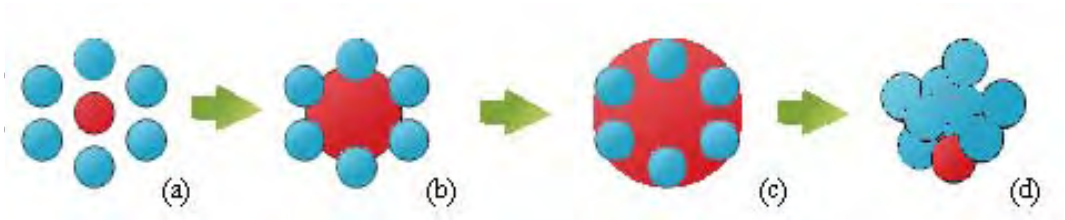


Figure 5-1: Evolving Dependency on Information

5.6 The Evolution towards the Information Age

As was indicated in the previous sections, information and the supporting information and communication technologies can no longer be divorced from the underlying business environment, as information is the glue that holds them together. Therefore, business and information risks need to be managed in an integrated way. From a business side of things, it is said that business departments operate in "silos" and that risk management also tended to be done in silos, with no concordance between these "silos". This is typically represented in figure 5-2 (a & b), where no or very little coordination existed between the departments. Figure 5-2, bottom row, indicates the evolution of the risk management process. The open circle indicate risk identification, the rectangle the processing of risk information, i.e. risk estimation and evaluation. The dark circle indicates the output of the risk identification, estimation and evaluation (refer to Section 2.4), internal controls.

Figure 5-2 (a) indicates a pre-computer-centric view, where no computer department was in existence; therefore, there was no need to perform computer-related risk management. The non-existence of an ICT department and its risk management is indicated by the faded part of figure 5-2 (a).

During the computer centric-era, when computers were introduced in the business environment, protection focused on hardware. Protecting it was as easy as locking a door because computers were standalone units and were not connected. Hence, computer risk management was considered to be a part of physical security (see Figure 5-2 b). Figure 5-2 (b) indicates that there is no coordination between the risk management practices, especially pertaining to ICT and others. During the IT-centric

era, computers were being connected to each other and the Internet, and it became possible to inflict harm via the corporate network or the Internet. Since organisations were so dependent on the computer infrastructure, any disruption would filter through and affect the business as well. It became extremely important to consider ICT risk management. However, some consideration should have been given to the various relationships between ICT and other risk management activities (see Figure 5-2 c), and this is indicated by the lines between the risk management processes. Currently, in the information age, where information is considered the lifeblood of an organisation, the trend is towards a more integrated risk management approach. Focus is placed on internal controls and the integration of the various departments (see Figure 5-2 d).

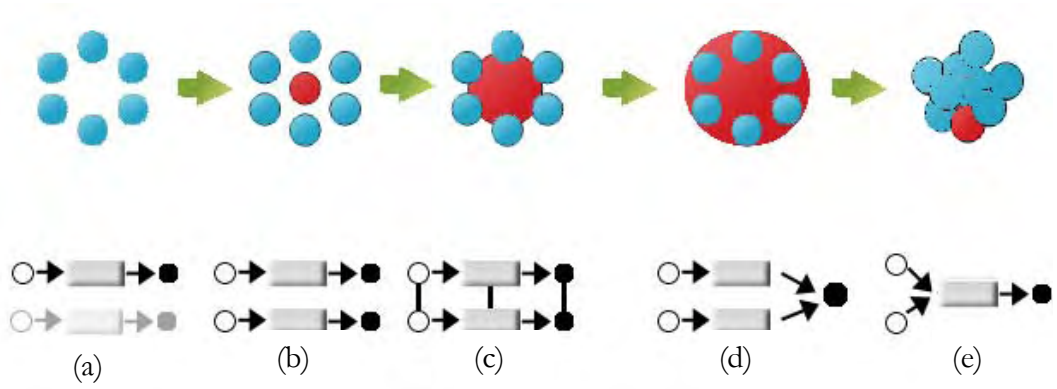


Figure 5-2: Risk Management along Evolution of Dependency on Information

To summarise, over the years, business has become more and more dependent on information, and thus the underlying infrastructure. Beyond the information age, from a business perspective, various departments are integrated and organisational lines are blurred. In this case, it only seems natural to have a much more integrated risk management approach. In such a case, the processing of risk decisions would be considering all risks and their relationships, taking a holistic, portfolio view of risk. See Figure 5-2(e). The importance of an integrated approach to information risk management will be reinforced in the next section when an analogy of the human body will be used.

5.7 Risk Management to Ensure a Quality Lifestyle

"Your body is the epicentre of your universe. You go nowhere without it. It is truly the temple of your mind and your soul. If it is sagging, softening, and aging rapidly, other aspects of your life will soon follow suit" (Phillips & D'Orso, 1999).

It can be argued that the human body is the 'vehicle' for individuals through life. All humans want to experience a quality life, and in order to live it, individuals need to have properly functioning vehicles for their journey.

However, what a 'quality life' entails does, of course, differ from person to person (Figure 5-3 a). Stephen Covey (1989) identified various centres in the lives of individuals. Some of these include family, money, pleasure, hostility, friendship, religious faith and self-centredness. For example, one person enjoys a quality life if he/she can perform exceptionally well on the sport field, and his/her whole life revolves around sport. For another person, a quality lifestyle could mean having a lot of money, and every action contributes to financial empire building. Yet another person's life could revolve around their family. Nonetheless, all human beings desire a quality life.

Normally, no matter what a person deems as a quality lifestyle, everyone requires a healthy body to experience it. A healthy, functioning body contains numerous systems that constitute it. These systems function and interact seamlessly and depend, to a large extent, on each other. As indicated in Figure 5-3 b & c, these systems holistically contribute to a quality lifestyle. Examples of these include the cardiovascular, digestive, nervous and muscular systems. Some of these have various sub-systems, for example, cardiovascular, which consists of a heart, arteries and veins, which are considered systems in their own right. All systems in the human body are integrated, interdependent, in synergy, and altogether more than the sum of its parts (Figure 5-3 c). An example of such integration and interdependence are the cardiovascular and respiratory systems, which together form the cardio-respiratory system.

This system's function is to ensure that the various organs and limbs receive the required amount of oxygen and consists of the heart, the lungs, the arteries, the veins and the blood. The lungs extract oxygen from the air and place it in the blood. The heart then pumps the blood through the arteries and veins to the various parts of the body. Notwithstanding, there is a great deal more to the system, such as transporting nutrients, waste products and hormones throughout the body and regulating blood pH and body temperature (Seeley, Stephens, & Tate, 1989). So, if the cardio-respiratory system's effective functioning is of the utmost importance to the well-being of the human body, so it is also to the quality of life.

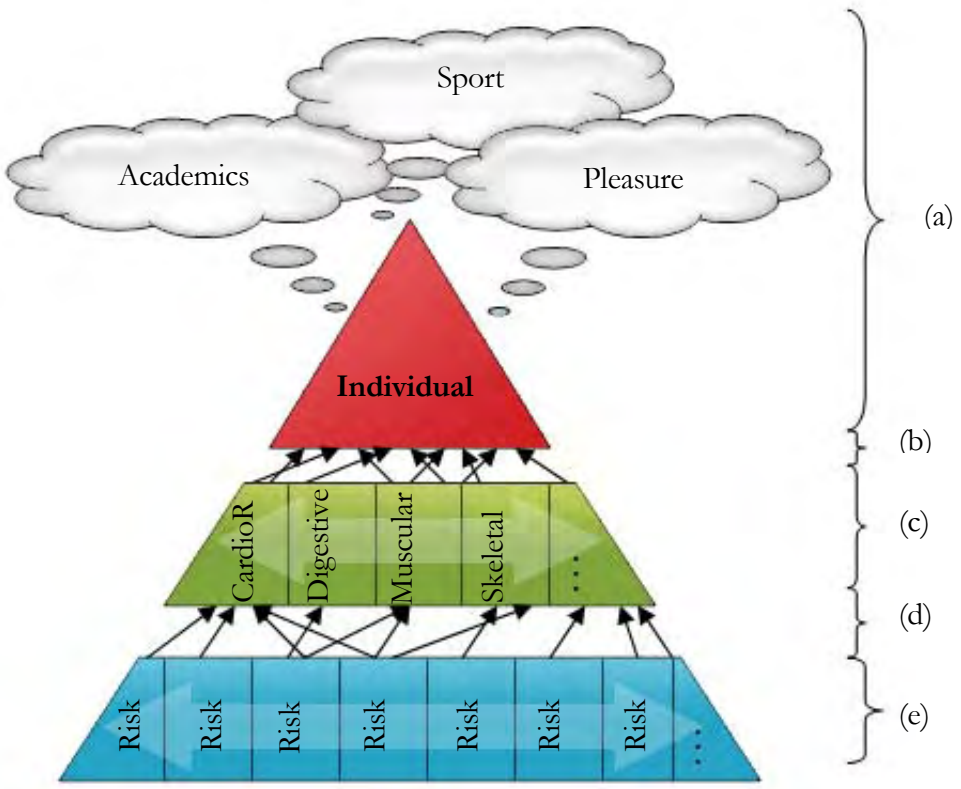


Figure 5-3: Bodily Risk Management

Risks, like injury and illness, could threaten all the systems or affect only one. However, if one system fails, others will soon follow suit. Eventually, the quality life of the individual, whatever it may be, is in jeopardy.

To ensure the proper working of the cardio-respiratory system, and ultimately ensuring a quality lifestyle, these risks should be managed. Typically, risk management activities include performing cardiovascular exercise, such as running or aerobics. This will give the whole cardio-respiratory system exercise and improve oxygen supply to the entire body. Another risk management activity may be eating the right foods, such as fresh fruit and vegetables, and avoiding fatty foods. This might help to prevent cancer and will certainly assist in controlling high, unhealthy cholesterol levels. On the contrary, there are activities that negatively influence the human body. An example of such a harmful activity that should be avoided is smoking, which may cause lung cancer. Furthermore, some risks fall outside the control of the individual, for example, hereditary disease. In addition, regular medical checkups are advised to monitor and evaluate the overall health situation.

It is important to note that all of these factors are interdependent. Exercising alone will not normally ensure a healthy heart, and it is possible that one could have a healthy heart but weak lungs, for example, which is not conducive to a healthy body or a quality lifestyle. Furthermore, some risks affect more than one organ or system, but some risk management practices can control more than one risk (see Figure 5-3 d & e). For example, a healthy diet will positively affect the digestive system, the cardiovascular system, the skeletal system, and most other systems in the human body.

If an individual falls ill, normally some risk materialises and influences one or other of the bodily systems. Although only one system may be malfunctioning, because of the ailment, the complete body will be influenced, and the individual will not enjoy a quality life whilst ill. Normally, in situations like this, the individual might visit a medical doctor who will examine the individual, diagnose the problem and prescribe some treatment. This should cure the ailment, ensure that the influenced system functions properly again and restore the health of the individual to again enjoy life.

Thus, it can be concluded that:

Quality of life depends on a healthy body;

- A healthy body depends on a set of properly functioning systems;
- These systems are all interdependent;
- Various risks threaten every system;
- If one of the risks materialises, it will have a negative effect on at least one of the systems with the result that the whole body will suffer and quality of life will be influenced;
- Risks are managed in a holistic way through exercise, healthy eating, not smoking, etc. The eventual goal is to ensure a healthy body that will enable a quality life;
- The aim of risk management is not to focus separately on individual systems, but rather to determine what is required to ensure a quality life and to ensure that a holistic, all-inclusive risk treatment plan is introduced to guarantee a healthy body and mind that, in turn, depends on properly functioning systems.

5.8 Risk Management from an Enterprise Perspective

The previous section discussed risk management as an integral exercise to ensure a quality lifestyle for a human being. It can be argued that an enterprise has a 'life', and that this enterprise also wants to maximise the quality of its lifestyle. This refers to its mission and vision (Figure 5-4 a). Enterprises can have different missions and visions, and a quality lifestyle can mean different things to different enterprises. Examples of these include profits, good working conditions, creating jobs, etc.

Similar to the human body, an enterprise consists of various systems. These departments, processes and systems operate interdependently, but most of them are linked to and dependent on IT systems. However, there are various risks threatening this synergy of systems, and these therefore also threaten the mission and vision of an enterprise. These should be properly managed in a holistic and all inclusive manner

(Figure 5-4). The rest of this section will compare an enterprise's 'life' and risk management to that of human beings.

It has been said that information is the lifeblood of an enterprise (Halliday *et al.*, 1996), with the heart and veins being the information and communication technology. Similar to the cardio-respiratory system, ICT systems are totally integrated and interdependent on the rest of the enterprise systems. The heart of the enterprise, the ICT department, pumps information (the blood) to and from processes and activities through the networks and communication channels, which can be considered the veins and arteries of the enterprise. As mentioned before, the digestive system absorbs nutrients from food and then transports them via the bloodstream. Similarly, various enterprise departments gather information that is then processed and transported horisontally and vertically through an enterprise. If information arrives at the right place at the right time, informed decisions can be made, and business processes can function. If this happens successfully, the enterprise is moving closer to reaching its mission and vision.

If something goes wrong with the heart, or if the veins are clogged-up with cholesterol, supplies of nutrients and oxygen will not reach the dependent systems effectively. If the enterprise's 'heart', the ICT department, is not functioning properly, information cannot be 'pumped' to the business systems where needed. Some processes that are totally dependent on information, might even cease to function. Nonetheless, if the heart is weak, it does not necessarily mean that the rest of the system will not function, but it will not function optimally. From an enterprise's perspective, if the ICT is down, the rest of the enterprise will also be impacted upon. The magnitude of the impact will rest on how dependent the enterprise is on ICT and will change from enterprise to enterprise.

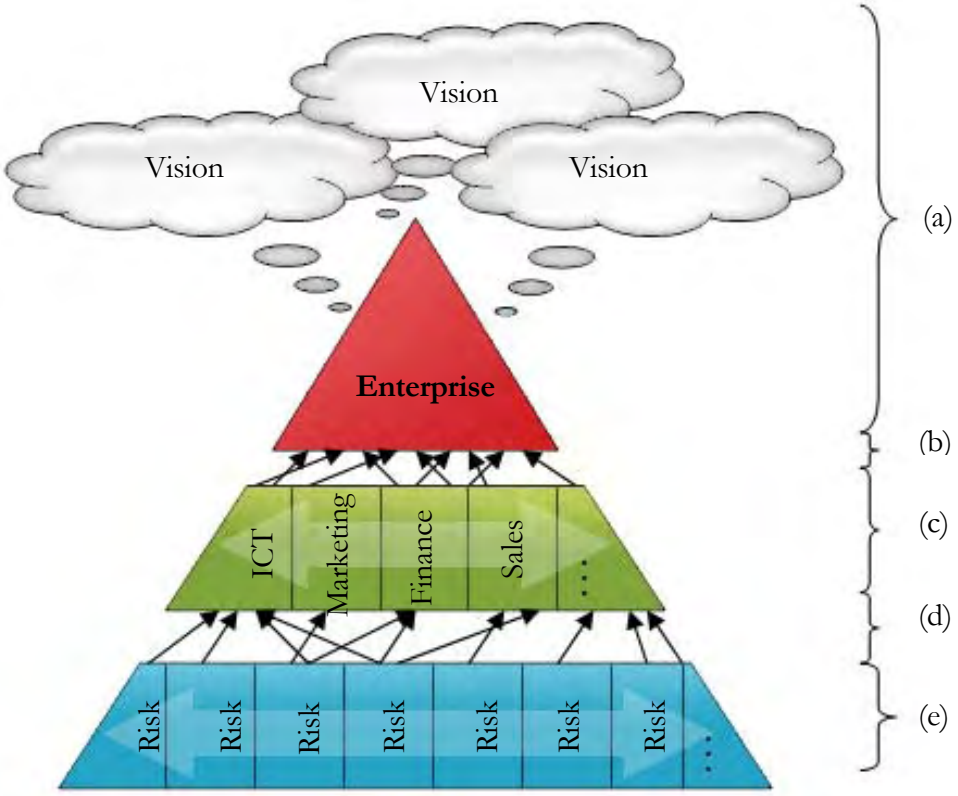


Figure 5-4: Risk Management from an Enterprise Perspective

A human being, who wants to ensure that his/her cardio-respiratory system functions optimally, has to continually manage his/her body well and even undergo a change of lifestyle, if necessary. In an enterprise, risks need to be managed as well. All human resources, from the board right through to the floor, need to adopt such an enterprise-wide risk management culture and take responsibility for risk management (King II, 2002).

In an enterprise, some risks threaten more than one system or department. Some risk measures that are taken may help cater for various risks and have an impact on more than one department (Figure 5-4 d). Additionally, risk management in an enterprise is not a once-off activity, but an ongoing process - a change in lifestyle. To establish and maintain such a process, discipline and dedication are required and these call for the corporate culture to adapt accordingly. Furthermore, an all-inclusive approach to risk

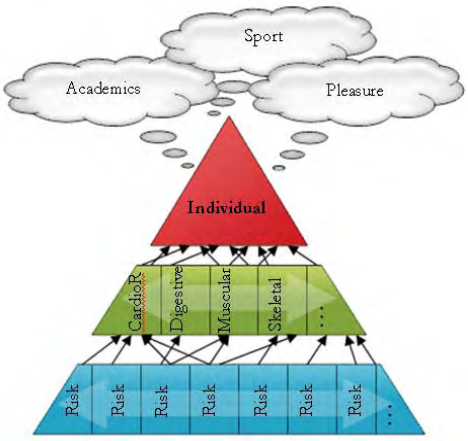
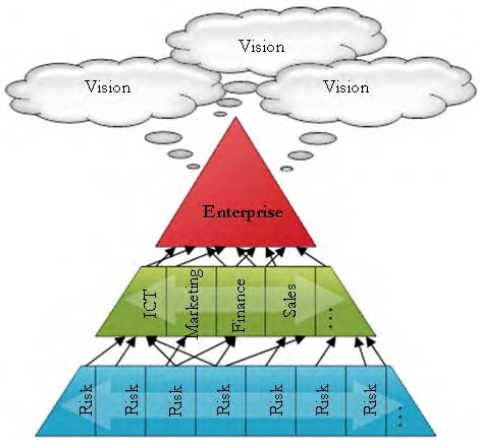
management must take place in all enterprise departments and systems, not just a select few.

If a human being falls sick, he/she seeks medical attention from a doctor, whereas in an enterprise this is done by a risk manager. Blakley, McDermott and Geer (2001) argue that information risk should be managed by professionals with similar characteristics as physicians. These include (Blakley *et al.*, 2001):

- Professional and specialised education;
- Licence to practice that can be revoked;
- Ethical obligation that they will handle their patients and their personal information with care;
- Professional obligation to handle and control adverse conditions by means of a prescription;
- Professional obligation to report on any relative and important information to the right authorities.

Table 5-1 provides a summary of all comparative arguments for qualities of life for both a human being and an enterprise.

Table 5-1: A Comparison of Risk Management from a Human and Enterprise Perspective

The human body	The enterprise
	
Quality life is ultimately the vision of the individual person.	A quality 'life' is ultimately the vision of any enterprise.
This quality life means different things to different people: it can be fame, money, sporting achievements, etc.	The quality life means different things to different enterprises, examples are financial success, creating jobs, being socially responsible, etc.
The quality life depends on the various systems of the body functioning effectively.	The quality life of the organisation depends on its various departments, systems and processes functioning effectively.
The function of the cardio-respiratory system is to make sure oxygen and other important nutrients get to where they are needed at the right time in the right quantity for individual systems to function.	The function of ICT is to make sure information arrives at the right time in the right format where it is needed for individual systems to function.
If the cardio-respiratory system and other systems function effectively, the individual can enjoy a quality life.	If the ICT and other systems function effectively, the enterprise can have a quality 'life'.
All systems, including the cardio-respiratory system, have risks that	All systems, including the ICT, have risks that threaten its well-being and

threaten it and ultimately threaten the well-being of the individual person.	ultimately threaten the well-being of the enterprise.
These risks need to be managed.	These risks need to be managed.
A doctor helps the individual manage his/her health risks, while it is ultimately the responsibility of the individual.	A risk manager helps the enterprise manage its risks, while it is ultimately the responsibility of everyone in the enterprise.
If all health risks are properly managed, the chances of a healthy working body and mind are increased, which means a quality life is possible.	If all business risks are properly managed the chances of a 'healthy', effective company is increased and a quality 'life' for the company is possible.
The risks associated with the cardio-respiratory system are not managed independently of the risks of other bodily systems.	The risks associated with ICT should not be managed independently of the risks of other systems.
The risk management process for the cardio-respiratory system is integral to the overall objective of the human being and, therefore, all risk management processes need to be integrated to ensure the objectives are reached.	The risk management process for the ICT system is integral to the overall objective of the enterprise and, therefore, all risk management processes need to be integrated to ensure the overall enterprise objectives are reached.

Today, enterprises must ensure that risks are managed holistically and that ICT-related risk terminology and practices are congruently aligned with those of the enterprise. The business environment and information technology are bound together by information (Eloff *et al.*, 1993). For this reason, it is imperative that risk management is synergised in the business, IT and information worlds. A thorough, all-inclusive risk analysis exercise needs to be conducted in business *and* supporting environments in order to develop an effective internal control system. Such an internal control system should reduce the exposure of risk and aid the safeguarding of assets (Cadbury, 1999). Indeed, in today's so-called information age, where business processes integrate the business and ICT environments, it is imperative that a unary internal control system be established, based on a holistic risk management exercise.

5.9 Defects of Information Risk Management

Up to this point, the importance of an integrated risk management process has been discussed by comparing risk management in the human body with that of enterprises. One of the things that have come to light is that risk management has been segmented based on enterprise departments and systems, is ad hoc and narrowly focused. The analogy earlier highlighted that risk management must be undertaken in a holistic manner. Therefore, it would be advantageous to integrate all these various risk management strategies.

A major problem being experienced in the business environment today is that enterprise risk cannot be managed effectively, because business and information-related risk are not congruently aligned with risk management terminology and practices. The business environment and information technology are bound together by information. For this reason, it is imperative that risk management is synergised in the business, IT and information worlds. A thorough, all inclusive, risk analysis exercise needs to be conducted in business *and* supporting environments in order to develop an effective internal control system. Such an internal control system should reduce the exposure of risk and aid the safeguarding of assets (Turnbull, 1999). Indeed, in today's so-called information age, where business processes integrate the business and IT environments, it is imperative that a unary internal control system be established, based on a holistic risk management exercise.

It is concluded that risk management used to be fragmented, ad hoc and narrowly focused. However, in this day and (information) age, it is necessary to move towards an integrated, holistic and continuous risk management process (Barton *et al.*, 2002). To achieve this, a model is required that will assist enterprises to manage information risk, while considering enterprise-wide needs.

5.10 Conclusion

For a human being to enjoy a quality life, a healthy body is a prerequisite. A healthy body cannot be achieved with a quick-fix pill; rather an all-inclusive, integrated risk

management approach is required. The resultant healthy body will enable an associated healthy lifestyle, and ultimately a quality life can be enjoyed. Similarly, ICT is, to a large extent, an enabler for a quality lifestyle of an enterprise and ultimately contributes towards the mission and vision of the enterprise. For the same reasons mentioned above, an all-inclusive, integrated, enterprise-wide risk management approach needs to be adopted. ICT cannot be seen any longer as a freestanding component as far as risk management is concerned. It should form part of a holistic, integrated enterprise risk management exercise that should ensure that the whole enterprise is 'healthy' to ensure maximum probability that the vision and mission can be met.

This chapter discussed the problem of discontinuity between the ICT and business environments. Even though enterprise risk management attempts to solve a very similar problem, no conclusive or exhaustive solutions have been offered on how to integrate ICT and information risk management. Additionally, corporate governance guidelines acknowledge the importance of risk management as well as information and communications technologies, but that is where it ends. A philosophy regarding integrated enterprise information risk management is introduced in the next chapter.

Section 4: Solution

Chapter 6

EPIRISMM: AN ENTEPRISE INFORMATION RISK MANAGEMENT MODEL

6.1 Introduction

From the previous chapter, it can be concluded that a model to assist with the holistic management of enterprise information risk would be appreciated by parties from business and ICT alike. Such a model will allow risk management to be enhanced by synergising the enterprise resources and risk activities. EPiRISMM, pronounced e-prism (Table 6-1), an enterprise information risk management model that meets all criteria highlighted earlier, will be discussed.

Table 6-1: EPiRISMM Acronym

EP	**E**nter**P**rise
i	**i**nformation
RIS	**RIS**k
M	**M**anagement
M	**M**odel

This chapter will start with the objectives of EPiRISMM. Next, arguments will be offered that present the crux of EPiRISMM. Thereafter, various models that can represent enterprise information risk management will be highlighted, and the final representation of the proposed model will be discussed. Subsequently, the steps used to employ EPiRISMM will be addressed. Finally, the conclusion will be offered.

6.2 EPiRISMM Objectives

Just as the shape of EPiRISMM has evolved, so has risk management over the years. The current situation is that there are various standards and best practices that all attempt to work towards a similar goal: the well-being of an enterprise. However, these publications are not congruently aligned, and some are in conflict with each other.

The ultimate goal of EPiRISMM is to offer a way to manage information-related risks as a subset of enterprise risk management. EPiRISMM will adopt, amongst others, the same objectives mentioned by Reynolds (2003) for a risk management framework. These objectives, along with others, are mentioned below:

- make it easy to comprehend and utilise integrated information risk management;
- represent how information, ICT, governance and enterprise-related matters come together;
- link risk management strategy to business strategy;
- assist enterprise-wide understanding of risk governance processes and help carry out business strategy;
- synergise the enterprise resources and risk activities to enhance risk management;
- establish noetic and dynamic risk boundaries to reflect a company's risk appetite;
- develop a framework to help align behaviours of individuals and business strategies; and
- synergise and combine risk-related resources throughout an organisation.

6.3 EPiRISMM: The Conceptual Model

To reiterate, in the human body, merely protecting the cardiovascular system is not enough; even protecting the cardio-respiratory system is not enough. While looking after this cardio-respiratory system, negligence of other systems could later negatively affect the efficiency of the cardio-respiratory system. The overall objective of the management of bodily risk is much broader than the protection of systems, but about the overall well-being of the human being. The same argument holds for information risk management, where information *and* other enterprise aspects should also be considered. EPiRISMM combines information and governance-related aspects while being salutary to the enterprise. Arguments to substantiate these statements will follow in this section.

As mentioned previously, information is the lifeblood of an organisation, flowing through the whole enterprise (Halliday *et al.*, 1996). Without quality and timely information, it is impossible for the enterprise to operate effectively. Thus, the value of information and the enterprise cannot be considered separately. Furthermore, information is dependent on ICT, and it would be impossible in our day and age for information to be used effectively without ICT. It can be argued that information is the glue that keeps the enterprise and ICT together (Eloff *et al.*, 1993). Thus, the enterprise environment and the ICT environment are inseparable (Figure 6-1). To make sure the enterprise, information and ICT environments operate free of the risks that threaten them, risks should be properly governed.

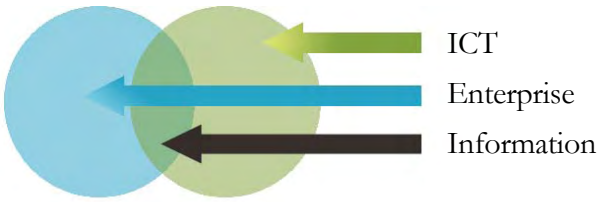


Figure 6-1: ICT and the Enterprise are Inseparable

Corporate governance "can, in part, be viewed as a company's strategic response to the need to assume prudent, appropriately mitigated risks, in exchange for measurable

rewards" (King II, 2002). Such rewards were mentioned earlier and referred to the mission or vision of the enterprise. In addition, 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" (Cadbury, 1999). From this is can be ascertained that corporate governance is an extremely important factor in the management of risk. Thus, corporate governance and enterprise environments are inseparable. Furthermore, it can also be argued that information is the glue that holds them together (Figure 6-2).

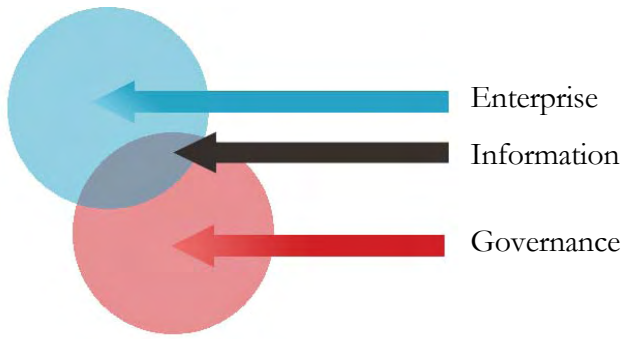


Figure 6-2: The Enterprise and Governance Aspects are Inseparable

In addition, governance is an important aspect in relation to ICT where it is important to properly govern information and related technology (IT Governance Institute, 2000). IT governance "enables the enterprise to take full advantage of its information, thereby maximising benefits, capitalising on opportunities and gaining competitive advantage" (The IT Governance Institute, 2000). These benefits mentioned by the IT Governance Institute can be related to the rewards mentioned earlier. This again points out that it is ultimately about the "communal goals", thus the overall well-being of the enterprise. Thus, ICT and governance environments are inseparable. Again, it can be argued that information is the glue that holds them together (Figure 6-3).

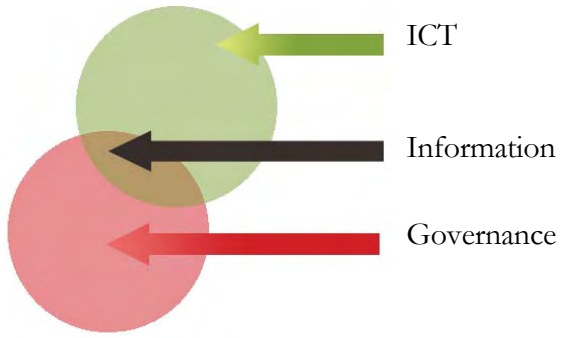


Figure 6-3: Governance and ICT Aspects are Inseparable

Figure 6-4 represents the relationship between information, governance, ICT and the enterprise. The top right circle represents the ICT department within an enterprise, the top left circle. Governance can be seen as an umbrella over the enterprise, and thus also over the ICT department. ICT is "pumping" information throughout the enterprise, and also to the governance "umbrella". However, these figures (Figures 6-1 through 6-4) do not imply that the ICT, Governance and the Enterprise only border with some overlap; rather, the enterprise overlaps them all but is represented as such for illustrative purposes only.

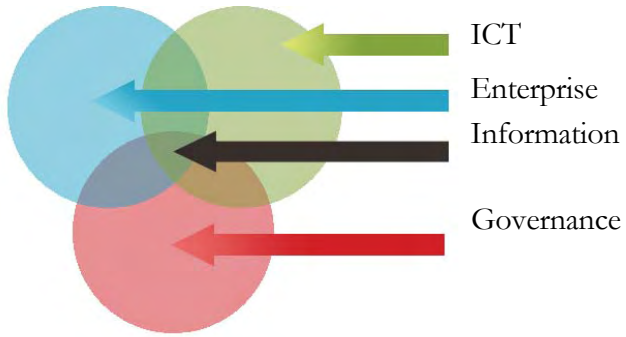


Figure 6-4: Relationship between Information, Governance, ICT and the Enterprise

From these statements, it can be concluded that quality information is dependent on the underlying ICT infrastructure and resources, sound governance principles and enterprise strategies. Thus, to effectively manage information-related risks, these three

aspects, i.e., ICT, governance and the enterprise, should be considered holistically, as depicted in Figure 6-4.

6.3.1 Development of a model

A model is needed to represent the integrated nature of the abovementioned aspects. The best way found to represent these aspects is as a prism. A brief history of the developments leading up to the prism will be offered in this subsection.

First a cubical shape was considered (Figure 6-5), which endeavoured to offer various perspectives of risk management from the three dimensions. However, information and ICT were considered one in this model, and this dissertation distinguishes between ICT and information (refer to Section 5.2). Because this model is attempting to solve a similar problem to COSO, this attempt seemed too close to the representation offered in the COSO ERM framework, which is also represented as a cube.

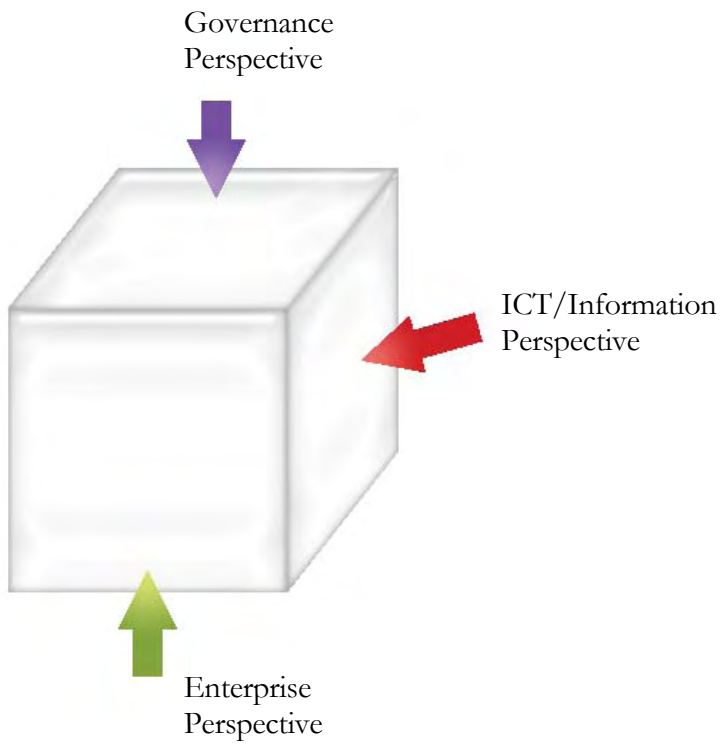


Figure 6-5: Draft Cubical Model Preceding EPiRISMM

Another draft conceptual model included the tripod/triangular pyramid. In this model (Figure 6-6), the three legs or sides also comprised ICT, governance and the enterprise, with quality information placed at the pinnacle. The idea behind the tripod description is that all three legs should be seen as equally important: if one leg fails or falls, the whole tripod will capsize. However, in this case, it seems that quality information is placed ahead of the enterprise as a whole. To avoid this perception, the prism conceptual model came to be, with information, governance and the enterprise being seen as mutually important, and thus with three equally long legs.

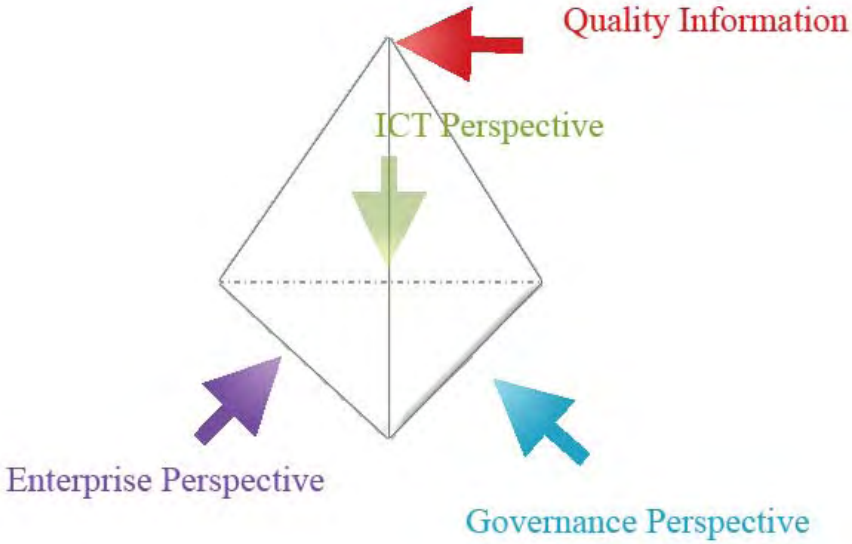


Figure 6-6: Pyramidical Model Preceding EPiRISMM

The schematic representation of these three aspects that influence the effective risk management of information is represented in Figure 6-7. Figure 6-7 only represents the top view of EPiRISMM. From now on, the sides of the model will be referred to as façades.

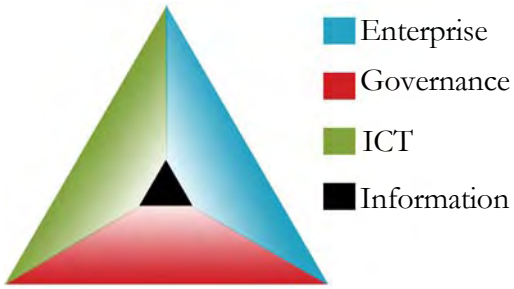


Figure 6-7: Top view of EPiRISMM

6.3.2 ICT

The ICT façade of the model refers to all information and communication technology aspects. The risks inherent in ICT should be properly managed. Risk management practices from an ICT perspective were discussed in Chapter 2 and will therefore not be discussed again in this chapter.

6.3.3 Governance

Earlier it was argued that governance is a critical aspect when it comes to risk management, and cannot be separated from ICT and the enterprise, therefore it makes up a façade of the model. From a corporate governance perspective, the board is responsible for providing the strategic direction to the enterprise. The King Committee of South Africa states that the board of directors is "responsible for the total process of risk management, as well as for forming its own opinion on the effectiveness of the process" (King II, 2002). King further elaborates on the responsibilities of risk management and states that all employees should take responsibility for risk management. This requirement will help ensure that the risk governance process is well comprehended in the enterprise. From the governance side, the general risk management strategy can be linked to the general business strategy, as mentioned earlier.

6.3.4 Enterprise

The enterprise side of EPiRISMM refers to the enterprise as a whole. Earlier it was highlighted that information plays a critical part in the success of an

enterprise. However, information is not the only aspect that is important, and there are many other aspects to consider. Examples of these include manufacturing of products, financial issues and human resource issues, but these fall outside the scope of this dissertation. Still, it is important to know that other aspects could be influential. Thus, the enterprise side can be seen as a link to various other organisational aspects.

6.3.5 Information

Information, which is dependent on ICT, critical to the enterprise and dependent on quality and sound governance principles, forms the core of the model. Furthermore, from the enterprise façade, the resources, including information, should be synergised with the various risk activities so that the management of risk is enhanced.

However, there is more to EPiRISMM than only two dimensions. EPiRISMM is broken down according to the three generic management levels, namely the strategic, tactical and operational levels (Figure 6-8), to form a three-dimensional prism (Kroon, 1996). Firstly, the strategic management level refers to long-term objective strategies. Furthermore, strategic management should develop a strategic vision, mission and goals for the enterprise. Secondly, the tactical management level refers to medium-term decisions, while management at these levels is required to transform the strategic vision into processes and functions. Lastly, the operational management executes processes developed by tactical management. Each of these levels requires different aspects from the management of risk. This three dimensional representation is given in Figure 6-9.

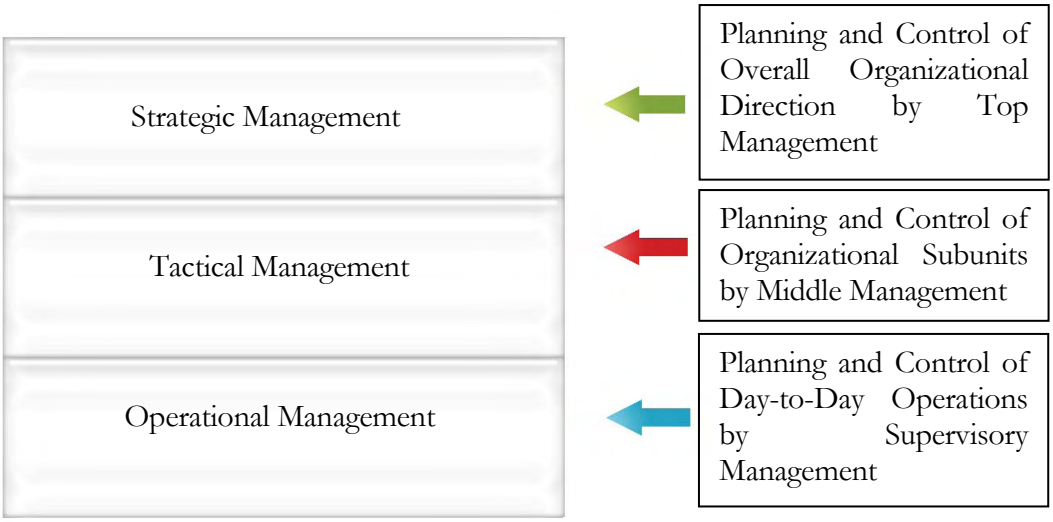


Figure 6-8: Management Levels

Figure 6-9 shows how all the aspects that have been discussed thus far come together. First, ICT, governance and the enterprise as a whole, with information being core can be observed from the top. Next, the model is broken down into strategic, tactical and operation levels. This will be used to indicate how information-related risk could be managed throughout the enterprise.

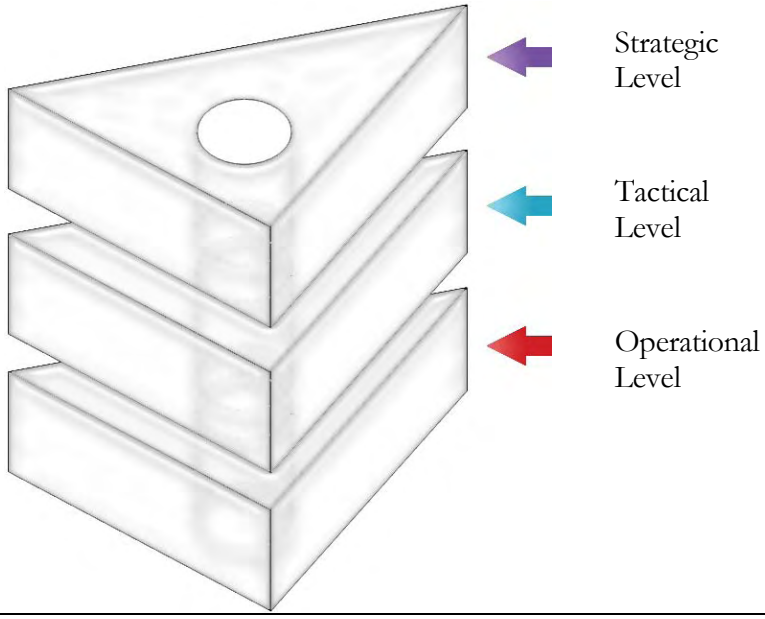


Figure 6-9: Three Dimensional Representation of EPiRISMM

6.4 Employing EPiRISMM

EPiRISMM has been established as a model that offers a holistic approach to enterprise information risk management. This section will discuss how the conceptual model can be used in order to obtain steps to manage information-related risks holistically.

The first step is to choose the correct set of guidelines, standards or best practices for governance, enterprise, ICT and information (Figure 6-10 a). The next step is to extract the activities or duties from the selected guidelines and place them in chronological order (Figure 6-10 b). Next, Rossouw *et al*'s (2003) view on the three managerial levels are used and the activities from the previous step are applied throughout the managerial levels (Figure 6-10 c). These are used to map the steps selected from the guidelines, best practices and standards to the three organisational levels. Finally, the output can then be used to holistically govern information-related risks throughout the enterprise.

6.5 Conclusion

This chapter centred around the problem described in Chapter 5 regarding the discontinuity of information risk management practices and put forward that to manage information-related risk effectively, enterprise, governance and ICT aspects must be considered holistically. A model called EPiRISMM was introduced to represent the amalgamation of these three aspects, and their relationship with information. It was revealed that information risk management can be applied at various levels of an enterprise, and therefore the model was broken down into the three managerial levels. Three steps were also discussed in this chapter that showed how the conceptual model can be used to arrive at certain activities that suggest to managers at the various levels how to manage information-related risks. The first step is to identify various publications on risk management from the abovementioned aspects which can be used together to manage information-related risks. The next step is to combine the publications and the third step is to apply the combined publications at the three organisational management levels. This acknowledges that there are

numerous standards, guidelines and best practices that are of good quality, but that they have to be integrated. EPiRISMM can in part be seen as a model that facilitates the mapping of these publications. The implementation of these steps will be discussed in the next chapter.

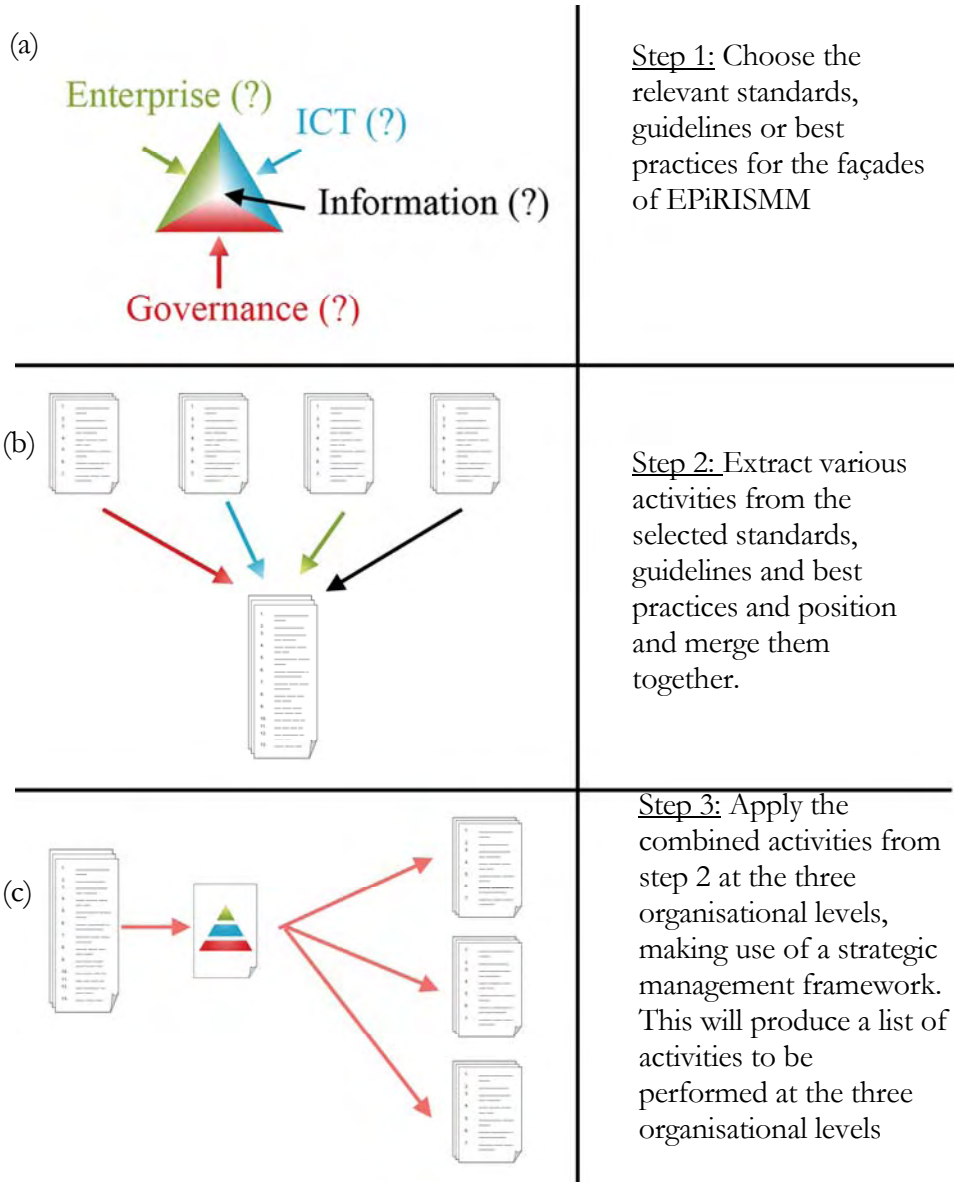


Figure 6-10: The Steps in EPiRISMM

Chapter 7

EPIRISMM: THE DETAILED MODEL

7.1 Introduction

In chapters 2 through 5, enterprise information risk management and the shortcomings thereof have been discussed. A conceptual model, EPiRISMM, has been proposed that will assist with these shortcomings by considering identified influences of information, i.e., ICT, governance and the enterprise, holistically. Various steps have been identified to employ the model and obtain various activities that must be performed at various levels in an organisation.

These steps will be discussed in this chapter. The first step to be discussed is the selection of relevant standards, best practices and guidelines for each of the façades of EPiRISMM. The next step is extracting various activities from the selected standards, guidelines and best practices, and mapping them together. Next, the final step to be performed is to apply the activities that have been identified at the various organisational levels. Finally, a conclusion will be offered.

7.2 Step 1: Selecting Relevant Standards, Best Practices and Guidelines

In Section 6.4, it was briefly stated that various standards or guidelines can be placed into the façades of EPiRISMM. This section will discuss each of the façades of EPiRISMM and the possible publications that may be placed therein.

7.2.1 Governance

From the governance perspective of EPiRISMM, numerous standards, guidelines and best practices may be applied. Examples of these include The Cadbury Report (Cadbury, 1999), The Turnbull Report (Turnbull, 1999), King I & II (1994; 2002) and The Sarbanes-Oxley Act (SOX, 2002). The King Report

focuses extensively on areas of risk management and internal control, while others, especially SOX, focus mostly on internal control, the process that follows on from risk management, both part of the management of risk (see Section 2.4). Because The King II Report is recently published, considered up-to-date and is internationally renowned it will be used for the input into the governance façade.

7.2.2 The enterprise

To fulfil the general enterprise requirements of EPiRISMM, enterprise risk management guidelines and standards will be considered. Examples of such frameworks and guidelines were covered in Chapter 4, and include the COSO ERM framework (COSO ERM, 2004b), The Grant Thornton Framework (Booker, 2003) and The Treasury Board of Canada's Integrated Risk Management Framework (Treasury Board of Canada, 2001). The COSO ERM framework is the most widely accepted of the frameworks discussed earlier, and is based on suggestions from participants' comments (Leitch, 2005). Therefore this framework will be adopted on the enterprise façade of EPiRISMM.

7.2.3 ICT

ICT is the third façade of EPiRISMM. Currently, there are a wide array of standards, frameworks and best practices that could be used to fulfil the ICT-related requirement of EPiRISMM, such as ISO 17799, ISO/IEC 13335 and NIST SP800:30. However, ISO 17799 addresses information as a whole, which includes ICT, and NIST SP 800:30 is too narrowly focused. For this reason, The ISO/IEC 13335 family will be used to fulfil EPiRISMM's ICT requirements.

7.2.4 Information

Information, "flowing through EPiRISMM", is core. This is very similar to ICT discussed above, as well as the standards, guidelines and best practices being used. ISO 17799 will be integrated into EPiRISMM because it focuses on information and not merely on ICT.

In the case where an organisation has specific needs or legislative requirements, the standards and guidelines discussed in this section may be replaced with more appropriate standards for the specific organisation. One such example may include replacing King (2002) with another country's governance guidelines to make it more relevant to that specific country. In another case, one set of guidelines may be replaced by a more recent set of guidelines, for example BS 7799:2 (2002) being replaced with ISO/IEC 27001 (2005) in recent years. Yet, in another case, more than one set of standards, best practices or guidelines may fit into a façade of EPiRISMM, supplementing each other. If the standards, best practices or guidelines are indeed replaced and EPiRISMM modified, it should be done by a person that has experience in risk management, and he/she should take care not to break the underlying philosophy of EPiRISMM.

7.3 Step 2: Extracting and Combining Activities

The previous section highlighted that four standards, best practices or guidelines, i.e. ISO 17799, COSO's ERM, the King Report and ISO 13335, could fit into the façades of EPiRISMM. This section will offer an overview of how the four standards and regulations integrate.

A study of the various standards, best practices and guidelines reveals various activities to be performed. Many of these steps are overlapping. Tables 7-1 to 7-4 show the steps within the four standards, best practices or guidelines that have been proposed earlier to fit into each façade of EPiRISMM. This representation does not attempt to be all-inclusive or portray the only way the steps can be interpreted, but is the interpretation of the author.

Table 7-1: Enterprise Activities Identified in COSO ERM

1. Apply enterprise risk management in setting strategy 2. Establish objective setting processes 3. Establish internal environment 4. Establish risk appetite and set risk tolerances 5. Identify potential events 6. Assess risk impact & likelihood

7. Identify and assess risk responses
8. Effect control activities
9. Inform & communicate with internal and external parties
10. Monitor the presence and functioning of other components of ERM

Table 7-2: Governance Activities Identified in King II

1. Define purpose of company
2. Determine values of the company
3. Identify stakeholders
4. Develop strategy by taking 1-3 above into account
5. Make sure that management implements the strategy mentioned in 4 above
6. Monitor implementation
7. Deal with the company's well known financial aspects
8. Identify key risk areas and key performance indicators
9. Determine how identified risks are managed
10. Ensure that the information that decisions are based on is reliable
11. Monitor human capital
12. Ensure strategic plans are effectively communicated
13. Ensure internal controls are effective and efficient

Table 7-3: Information Activities Identified in ISO 27001

1. Define ISMS scope and policy
2. Management of risk
3. Implement management programme
4. Implement selected controls
5. Manage operations and resources
6. Implement control procedures and processes
7. Execute procedures
8. Review residual risk and effectiveness of ISMS
9. Execute management procedures
10. Undertake formal review of ISMS regularly
11. Record & report all actions and events
12. Measure performance of ISMS
13. Identify improvements and implement it
14. Take appropriate actions
15. Communicate results
16. Revise ISMS and monitor revisions

Table 7-4: ICT Activities Identified in ISO/IEC 13335

1. Determining organisational ICT security requirements
2. Determining organisational ICT security objectives, strategies and

policies
3. Identifying roles and responsibilities within the organisation
4. Development of the ICT security plan
5. Risk assessment
6. Risk treatment decisions and safeguard selection
7. Business continuity planning
8. Implementing safeguards
9. Approval of ICT systems
10. Developing and implementing a security awareness program
11. Reviewing and monitoring the implementation and operation of safeguards
12. Configuration control and change management
13. Review, audit and monitoring, and security compliance checking
14. Information security incident management

By integrating and combining the above-mentioned activities (Tables 7-1 to 7-4), the following resultant series of steps can be derived:

Table 7-5: Combination of ISO 13335, ISO 17799, King II and COSO ERM

1. Define purpose of company	Table 7-2 Activity 1
2. Determine values of the company	Table 7-2 Activity 2 Table 7-4 Activity 1
3. Establish risk appetite and set risk tolerances	Table 7-1 Activity 4
4. Identify stakeholders	Table 7-2 Activity 3
5. Establish objective setting processes	Table 7-1 Activity 2
6. Develop strategy	Table 7-2 Activity 4 Table 7-1 Activity 1 Table 7-4 Activity 2
7. Establish internal environment	Table 7-1 Activity 3 Table 7-3 Activity 3 Table 7-4 Activity 3
8. Deal with well known financial aspects	Table 7-2 Activity 7 Table 7-3 Activity 3
9. Formulate policies	Table 7-3 Activity 3 Table 7-4 Activity 2
10. Risk identification	Table 7-1 Activity 5 Table 7-2 Activity 8 Table 7-3 Activity 2 Table 7-4 Activity 5
11. Risk estimation	Table 7-1 Activity 6 Table 7-3 Activity 2

12. Risk evaluation	Table 7-1 Activity 6 Table 7-3 Activity 2
13. Identify and assess risk responses	Table 7-1 Activity 7 Table 7-2 Activity 9
14. Risk treatment decisions and safeguard selection	Table 7-1 Activity 8 Table 7-3 Activity 4 Table 7-4 Activity 6 Table 7-4 Activity 8
15. Business continuity planning	Table 7-4 Activity 7
16. Develop ICT security plan	Table 7-4 Activity 4
17. Development of security awareness programme	Table 7-4 Activity 10
18. Manage operations and resources	Table 7-3 Activity 5
19. Implement control procedures and processes	Table 7-3 Activity 6
20. Execute procedures	Table 7-3 Activity 7
21. Approval of ICT systems	Table 7-4 Activity 9
22. Ensure lower management implements the strategies selected or developed	Table 7-2 Activity 5 Table 7-2 Activity 6 Table 7-4 Activity 11 Table 7-4 Activity 13
23. Ensure that the information decisions are based on, are reliable	Table 7-2 Activity 10
24. Review levels of residual risk	Table 7-3 Activity 8
25. Monitor the presence and functioning of other components of ERM	Table 7-1 Activity 10
26. Monitor human capital	Table 7-2 Activity 11
27. Ensure internal controls are effective and efficient	Table 7-2 Activity 13 Table 7-3 Activity 9
28. Measure performance of ISMS	Table 7-3 Activity 12
29. Configuration control and change management	Table 7-4 Activity 12
30. Review, audit and monitoring, and security compliance checking	Table 7-3 Activity 10 Table 7-4 Activity 14
31. Take appropriate actions	Table 7-3 Activity 13 Table 7-3 Activity 14 Table 7-4 Activity 15
32. Revise and monitor revisions	Table 7-3 Activity 16
33. Communicate with stakeholders	Table 7-3 Activity 15 Table 7-1 Activity 9
34. Ensure strategic plans are effectively communicated	Table 7-3 Activity 12
35. Record and report all actions and events	Table 7-3 Activity 11

This section discussed the second step in EPiRISMM which is to identify, integrate and combine activities from the publications that have been selected in step 1. The next section will discuss the third and final step, which is to apply the selected activities at the various organisational levels.

7.4 Step 3: Applying Activities at Various Organisational Levels

By further refining the above-mentioned activities, they can be reused at the various management levels mentioned earlier, i.e. strategic, tactical and operational levels. Rossouw, *et al* (2003) describe an approach for strategic management that breaks down the three levels of management further. This approach is summarised in Table 7-6. For this approach, the mission and other aspects are not merely a strategic concern, but should be implemented at lower levels as well.

Table 7-6: Levels of Management

1. Strategic level
    a. Develop a vision
    b. Develop a mission statement
    c. Determine values of the enterprise
    d. Do a SWOT-analysis
    e. Formulate strategic goals
    f. Do a gap analysis
    g. Identify generic and corporate strategies
    h. Evaluate and select strategies
    i. Review structure, leadership and culture
    j. Formulate policies
    k. Do strategic control
2. Tactical level
    a. Develop a mission statement
    b. Do SWOT-analysis
    c. Formulate tactical objectives
    d. Do a gap analysis
    e. Formulate tactical strategies
    f. Review policies
    g. Do tactical control
3. Operational Level
    a. Formulate operational objectives
    b. Formulate operational strategies
    c. Lead the team
    d. Do operational control

Finally, by combining the approach described by Rossouw *et al* (2003) in Table 7-6 with the combination of ISO 17799, the ISO/IEC 13335 family, King II and the COSO ERM framework suggested in Table 7-5, the following approach, described in Table 7-7, Table 7-8 and Table 7-9 could be derived.

Table 7-7: Activities from Table 7-5 Applied on those of Table 7-6

1. Strategic level
    a. Develop a vision
    b. Develop a mission statement
    c. Determine values of the enterprise
    d. Establish risk appetite and set risk tolerances
    e. Identify stakeholders
    f. Do a SWOT analysis
    g. Formulate strategic goals
    h. Do a gap analysis
    i. Identify generic and corporate strategies
    j. Evaluate and select strategies
    k. Review structure, leadership and culture
    l. Deal with well known financial aspects
    m. Formulate policies
    n. Management of risk (Section 7.4.4)
    o. Do strategic control (Section 7.4.5)
    p. Communicate (Section 7.4.6)
2. Tactical level
    a. Develop a mission statement
    b. Identify stakeholders
    c. Do SWOT analysis
    d. Formulate tactical objectives
    e. Do a gap analysis
    f. Formulate tactical strategies
    g. Review structure, leadership and culture
    h. Review/develop/implement policies
    i. Management of risk (Section 7.4.4)
    j. Do tactical control (Section 7.4.5)
    k. Communicate (Section 7.4.6)
3. Operational Level
    a. Formulate operational objectives
    b. Formulate operational strategies
    c. Review/develop/implement policies
    d. Management of risk (Section 7.4.4)
    e. Lead the team
    f. Do operational control (Section 7.4.5)
    g. Communicate (Section 7.4.6)

The three managerial levels to this point, and the tasks associated with them have been discussed. The following subsections will discuss each of these activities in more detail.

7.4.1 Strategic duties

The first strategic duty of any enterprise is to develop its vision (Table 7-7, Activity 1 a). King II (2002) describes this as defining the purpose of the company. An example of such a vision is that of Martin Luther King, when he stated: "I have a dream". That dream shaped the future of the United States. Similarly, the vision of the enterprise should shape its future and reflect the "visionary goals" of the enterprise (Sutherland & Canwell, 2004), of where the enterprise wants to go and how to get there (Kroon, 1996).

Next, a mission statement should be developed by considering the vision statement (Table 7-7, Activity 1 b). The mission statement is considered the "fundamental, unique purpose that sets the organisation apart from other organisations of its type and identifies the scope of its operations in … product, … market and … technological terms" (Brevis, Vrba, & de Klerk, 1997). Next, values are developed (Table 7-7, Activity 1 c), based on the mission statement, and are ideals that are accepted by the enterprise. Values determine what a person or enterprise considers as right or wrong. Moreover, values are influenced by emotions and reflects the culture of the enterprise (Rossouw *et al.*, 2003). An important value to consider is the risk appetite of the enterprise (Table 7-7, Activity 1 d), that is how tolerant the enterprise will be towards risk. COSO (2004b) mentions the articulation of risk management and risk tolerances only after the establishment of the internal environment; however it is essentially a value of the enterprise. The risk appetite may already be reflected in the vision of the enterprise.

The abovementioned steps, i.e., developing a vision, mission, and determining the value may not necessarily be part of risk management, but is ultimately, what the enterprise is about. In essence, risk management protects the enterprise on

its journey (mission) towards its destination (vision), and therefore will be included in EPiRISMM.

The next step is to identify key stakeholders (Table 7-7, Activity 1 e). Stakeholders include more than only the shareholders, and include the community, government and employees (Naidoo, 2002). Because the various stakeholders need to be considered during the SWOT analysis, identification is done before performing it. By performing a SWOT analysis (Table 7-7, Activity 1 f), the enterprise's external environment is scanned for opportunities and threats, while strengths and weaknesses are identified internally.

Formulating the strategic goals/objectives (Table 7-7, Activity 1 g) involves assigning numbers to the sought after results and attempts to "achieve the greatest output with the smallest input" (Kroon, 1996). Again, these goals must be congruently aligned with the enterprise's mission and vision statements. It is extremely important that an enterprise first establish its objectives before it manages risk, because risks are standing in the way of the enterprise reaching its objectives, and ultimately its vision (COSO ERM, 2004a). During the gap analysis (Table 7-7, Activity 1 h), the void between the sought after goals and the predicted outcomes are analysed (Rossouw *et al.*, 2003). This allows management to find generic and corporate strategies (Table 7-7, Activity 1 i) to align the forecasts with the strategic goals. In other words, the strategies must help the enterprise achieve its goals or objectives. The generic strategy may be based on the Ansoff (1986) Matrix (Figure 7-1), which consists of market penetration, product development, market development and diversification strategies. Corporate strategies on the other hand, include strategies such as innovation, horisontal integration and consortiums, amongst others. Once the enterprise knows about all the possible strategies, one of them should be selected. When considering the various strategies, the enterprise may make use of various techniques that enable the selection of the best-suited corporate strategy (Table 7-7, Activity 1 j). An example of such a technique is the *industry attractiveness-*

business strength matrix (Rossouw *et al.*, 2003). The various strategies that the enterprise may select have different levels of risk associated with them (COSO ERM, 2004b). The overall attitude of the enterprise towards risk also plays a major role in the selection of strategy, with the risk appetite of the enterprise being a major driver.

The next step is to review the organisational structure, leadership and culture (Table 7-7, Activity 1 k). Because structure is about the improvement of the effectiveness of an organisation by dividing the duties according to tactical units, it is critical to align the organisation's structure with its strategy. Leadership should be reviewed to ensure that top management is capable of implementing strategy, as well as ensuring that management is capable of handling complexity (Rossouw *et al.*, 2003). The culture should be reviewed and aligned with the enterprise's strategy and risk appetite.

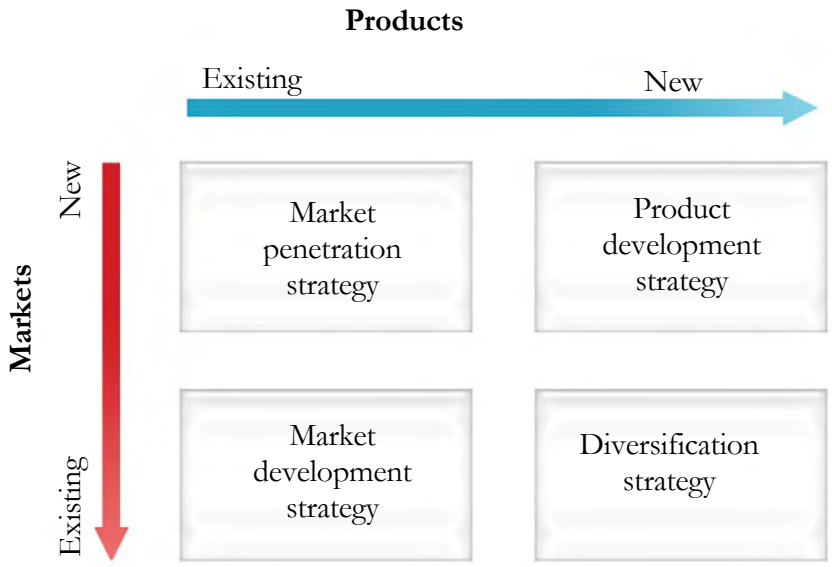


Figure 7-1: The Ansoff Matrix

Although the strategic level may not be responsible for some of the steps outlined here, it may ultimately be held accountable to the stakeholders for any

lack thereof. Next, the board should deal with well-known financial aspects such as budgets, which may include risk management-related aspects (Table 7-7, Activity 1 l).

Next, the development of strategic policies is listed (Table 7-7, Activity 1 m, Figure 7-2). However, the development of these policies is not limited to only after activity 13 because it is constantly being developed as other activities are being completed. Examples of these policies include the corporate business policy, derived from the objectives and strategy (ISO/IEC 13335-1, 2004). From the corporate business policy, the corporate security policy, corporate IT policy and corporate marketing policy, amongst others, are derived. Thereafter, the corporate information security policy is derived from these. In addition to the ICT-related policies, the information and information security policies may also be developed at a strategic level.

After some policies have been formulated, various activities follow that can be described and grouped as the management of risk (Table 7-7, Activity 1 n; Table 7-8), strategic control (Table 7-7, Activity 1 o; Table 7-9) and communicate (Table 7-7, Activity 1 p; Table 7-10). These will be discussed in the following sub-sub-sections.

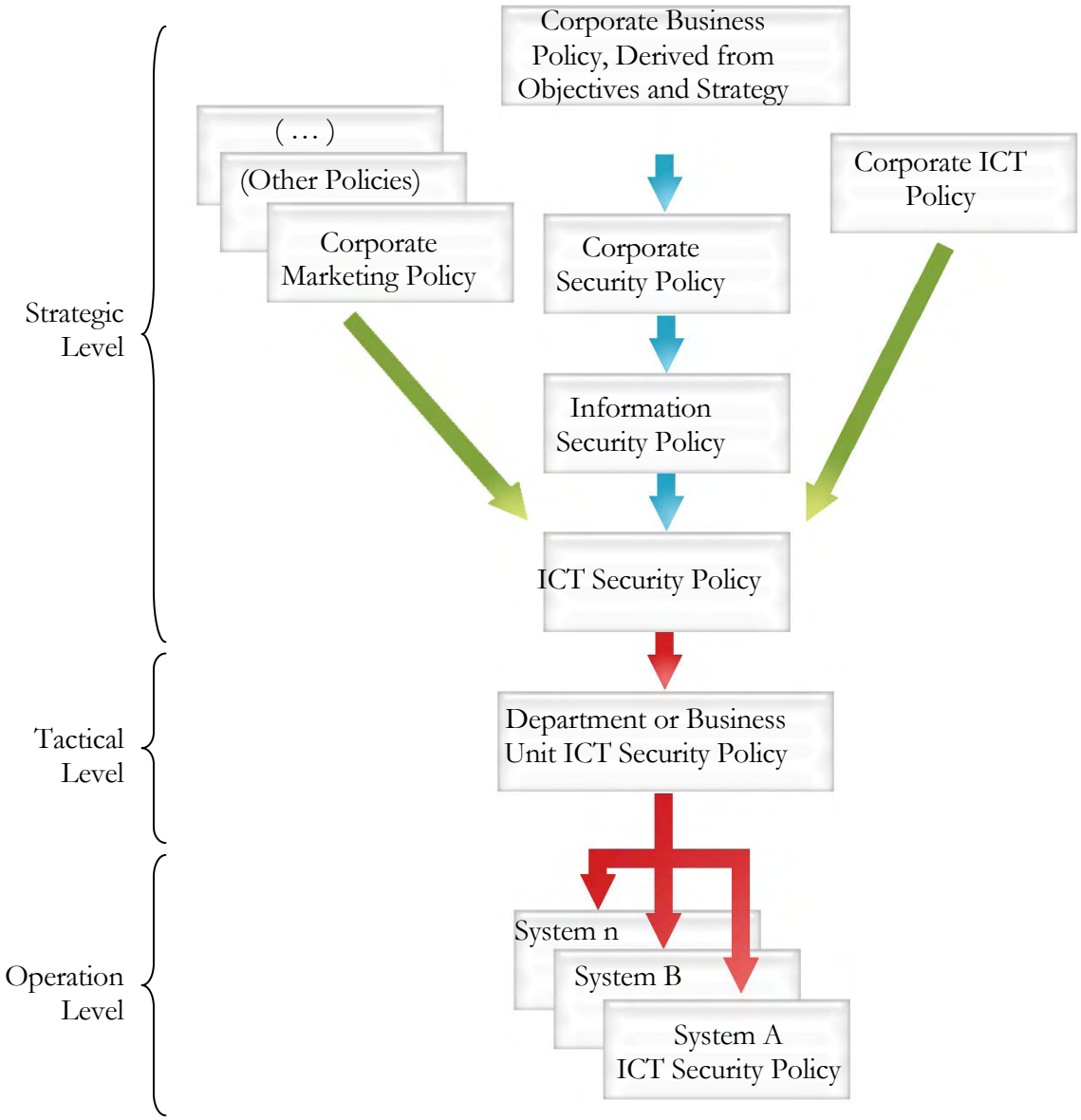


Figure 7-2: Policy Hierarchy

7.4.2 Tactical duties

Ultimately, the tactical level management must transform the strategic vision into processes and functions, as discussed in section 6.3. The tactical level duties are very similar to the strategic level duties, but the focus changes somewhat and is more granular.

Developing a tactical mission statement is focused on the tactical unit or department and should be in line with the overall (strategic) mission, as well as the vision of the enterprise (Table 7-7, Activity 2 a). Again, the stakeholders should be identified (Table 7-7, Activity 2 b), where after a tactical level SWOT analysis is performed (Table 7-7, Activity 2 c). The internal environment that must be considered in this case, for identification of strength and weaknesses, is only within the tactical unit or department (Rossouw *et al.*, 2003). Everything outside the tactical unit, even within the enterprise, is considered the external environment, which in turn, is used to identify opportunities and threats.

Next, the tactical objectives, also known as functional objectives are formulated (Table 7-7, Activity 2 d). These are medium term objectives (Rossouw *et al.*, 2003), typically one to five years (Kroon, 1996). Again, the objectives must be in line with the tactical mission, which will ensure that the tactical objectives are ultimately in line with the vision of the enterprise, assuming the tactical vision is in line with the strategic mission and vision. Following the formulation of objectives, the forecasted future situation must be compared with the objectives, and the tactical gap must be identified (Table 7-7, Activity 2 e). Thereafter, tactical strategies must be formulated to close the gap, which will ultimately help the enterprise achieve its vision (Table 7-7, Activity 2 f).

The structure, leadership and culture is reviewed next at the tactical or business unit level (Table 7-7, Activity 2 g). Next, strategic policies are revisited, and new, tactical policies formulated (Table 7-7, Activity 2 h). These policies must be in accordance with the strategic policies. As mentioned previously, policies are not just limited to this position (Table 7-7, Activity 2 h), because policies can be seen as a way to reduce the identified risks. The next activity listed is the management of risk (Table 7-7, Activity 2 i), which is covered in Section 7.4.4, followed by performing tactical control (Table 7-7, Activity 2 j; Section 7.4.5), and communication (Table 7-7, Activity 2 k; Section 7.4.6).

7.4.3 Operational duties

Finally, the operational level management, also known as first line management or supervisory management, will execute the processes and functions created by strategic management, as discussed in Section 6.3. The first listed activity is the formulation of operational objectives (Table 7-7, Activity 3 a). These objectives are aimed at the short term (Rossouw *et al.*, 2003), typically less than one year (Kroon, 1996). This should be in line with the tactical objectives.

The next activity is the formulation of operational strategies, which are sometimes called action plans (Table 7-7, Activity 3 b). These operational strategies must help the operational unit reach its objectives. The next activity is to review, develop and implement policies (Table 7-7, Activity 3 c), which is followed by the management of risk (Table 7-7, Activity 3 d). Refer to Section 7.4.4 for the management of risk. Next, the operational team should be lead (Table 7-7, Activity 3 e), and the first-line manager needs "to direct their staff and other resources so that they can, as a team, achieve the section's operational objectives" (Rossouw *et al.*, 2003). The last two activities are to do operational control (Table 7-7, Activity 3 f), discussed in Section 7.4.5, and communication (Table 7-7, Activity 3 g), discussed in Section 7.4.6.

7.4.4 Management of risk

The risks facing the enterprise at the strategic level must be identified, estimated and evaluated (Table 7-8, Activities 1 - 3). At the strategic level, the upside of risks is most evident, and this must be considered as well. The strategic risks are high-level risks, and techniques such as Top 10 Risk Tracking can be used. The lower down in the organisation, the more detailed the risk analysis becomes.

Table 7-8: Management of Risk Activities

1. Risk identification
2. Risk estimation
3. Risk evaluation
4. Identify and assess risk responses
5. Risk treatment decisions and safeguard selection
6. Business continuity planning
7. Develop ICT security plan
8. Development of security awareness programme
9. Manage operations and resources
10. Implement control procedures and processes
11. Approval of ICT systems

When an organisation is cognisant of the risks that face it, it is able to identify and evaluate risk responses (Table 7-8, Activity 4). This is done by identifying and selecting possible risk response strategies, as discussed in Section 2.7.4, i.e. acceptance, avoidance, mitigation or transference.

Thereafter, risk treatment decisions are made and safeguards are selected (Table 7-8, Activity 5). This will include the implementation of controls and safeguards, such as those described in Table 2-2, including planning for business continuity (Table 7-8, Activity 6), developing the ICT security plan (Table 7-8, Activity 7), as well as the development of various policies and procedures. Procedures are developed to state how policies must be implemented (Barman, 2001). An example of such a procedure is the ICT security plan which describes how to secure ICT assets (Table 7-8, Activity 7), and in turn may require the development of a security awareness programme (Table 7-8, Activity 8). The ICT plan may only be developed and implemented at lower levels. However, depending on the organisation, this may be done at the strategic level already.

Again, according to section 6.3, policies and procedures are tactical level activities, but can differ depending on the organisation. Next, the operations and resources should be managed (Table 7-8, Activity 9), especially with regard to the Information Security Management System (ISMS), and procedures that have been developed must be executed (Table 7-8, Activity 10). The approval of ICT

systems, although not directly related to risk management will fall in here (Table 7-8, Activity 11), and again depends on the organisation.

7.4.5 Monitoring activities

The monitoring activities are next, which involves regular checking of the activities mentioned above (Table 7-9). This is referred to as strategic control (Table 7-7, Activity 1 o), tactical control (Table 7-7, Activity 2 j), and operational control (Table 7-7, Activity 3 f) which "involves following up the strategy as it is implemented, identifying problems or changes in the underlying assumptions, and carrying out the necessary adjustments" (Rossouw *et al.*, 2003). One example of such monitoring is that strategic level management must ensure that the lower levels of management implement what is required of them (Table 7-9, Activity 1). The same is true for tactical level management, while operational management must see to it that policies and procures are implemented and followed at ground level. Other examples of such monitoring activities include ensuring that the information decisions are based on is reliable (Table 7-9, Activity 2), review levels of residual risk (Table 7-9, Activity 3), monitor the presence and functioning of other components of ERM (Table 7-9, Activity 4), monitor human capital (Table 7-9, Activity 5). Internal controls must also be monitored and strategic management must ensure that it is effective and efficient (Table 7-9, Activity 6). The performance of the ISMS must be monitored (Table 7-9, Activity 7) and configuration control and change management must be done (Table 7-9, Activity 8). Periodic reviews and audits, as well as compliance checking must be conducted to ensure its effectiveness (Table 7-9, Activity 9).

When irregularities or ineffectiveness is spotted, appropriate corrective actions should be taken which (Table 7-9, Activity 10), in turn, must also be revised and monitored (Table 7-9, Activity 11).

Table 7-9: Monitoring Activities

1. Ensure lower management implements the strategies selected or developed
2. Ensure that the information decisions are based on is reliable
3. Review levels of residual risk
4. Monitor the presence and functioning of other components of ERM
5. Monitor human capital
6. Ensure internal controls are effective and efficient
7. Measure performance of ISMS
8. Configurations control and change management
9. Review, audit and monitoring, and security compliance checking
10. Take appropriate actions
11. Revise and monitor revisions

7.4.6 Communications

The last activity for the three levels is communication (Table 7-7, Activity 1 p, Activity 2 k and Activity 3 g). The various stakeholders must also be kept informed of what is happening throughout the enterprise (Table 7-10, Activity 1). Therefore it is important to record all relevant actions and events (Table 7-10, Activity 2). This include making available the risk management practices of the enterprise as required by King II (2002). Internal communication must also take place to communicate strategic and other plans to the necessary staff (Table 7-10, Activity 3).

Lastly, it is important to emphasise that various communications activities followed must take place during all the above-mentioned steps. However, these activities should not be limited to only this segment, but communication should happen during all activities.

Table 7-10: Communication Activities

1. Communicate to stakeholders
2. Ensure strategic plans are effectively communicated
3. Record and report all actions and events

This section described the third step of EPiRISMM, which was to orchestrate the activities identified in the second step based on the management levels and activities by Rossouw *et al* (2003). These activities at the various organisational levels were then discussed.

7.5 Conclusion

This chapter discussed the execution of the three steps indicated in Figure 6-10. Firstly, standards, guidelines and best practices were chosen for the three façades and core of EPiRISMM. Within each of these, various activities were identified and these were then synthesised, where after it was applied to the various organisational levels. It can be observed that policies are not just articulated at one place in each level, but throughout the enterprise. This, of course, would differ from one enterprise to another. The next chapter will offer a case study to indicate how EPiRISMM could be applied in a real world situation.

Chapter 8

EVALUATING EPIRISMM

8.1 Introduction

Chapter 6 introduced a model, EPiRISMM, to illustrate how information-related risks could be managed. It introduced three steps to implement it. Thereafter, Chapter 7 followed these steps introduced in Chapter 6 and identified various activities that can be used to manage information-related risks holistically.

However, EPiRISMM is strongly founded on theory and therefore, this chapter aims to 'test' EPiRISMM by making use of a case study. First, the company will be described, where after the implementation of EPiRISMM at this company will be described. Thereafter, findings and suggestions to improve EPiRISMM will follow and finally, the conclusion will be offered.

8.2 Nature of the Case Study

EPiRISMM has to be evaluated or tested in some form, and it was decided that a case study would be most effective for this task. However, because of the extent of EPiRISMM, as well as the levels at which it can be applied, it was be difficult to find a suitable enterprise that would be willing to assist with such a case study. Moreover, to implement such a case study would take up too much time. Therefore, it was decided to apply EPiRISMM at a smaller enterprise. The information used in this case study is based on a real business, which wants to remain anonymous. This organisation will be referred to as XYZ.

8.3 Company XYZ Profile

XYZ is a relatively new IT company that was established in 2003. It believes that small - medium sized businesses are the backbone of most modern-day economies, and that

they are characteristically run and managed by their owners, who either do not possess all the necessary qualifications, or do not have the time to fulfill the necessary business functions. XYZ wants to fulfill the IT requirements of these companies by offering e-marketing strategies. XYZ's mission is as follows:

> "We aim to be the preferred internet marketing service provider for small - medium sized businesses who wish to concentrate on their core competencies by outsourcing their IT and IT-marketing functions. We achieve this by becoming your business-partner, offering expert, cost effective e-marketing and IT business solutions".

XYZ currently has less than 20 employees that serve its clients. The company is structured according to the services and products that it offers. The products are currently divided into three main categories, described as technical, business and software. The technical services include domain registration, search engine optimisation and Internet connectivity. Next, the business services offered include e-marketing, including web development, and strategic business management consulting. Lastly, XYZ offers software sales and support, new product development and web-application development.

Currently, the strongest area of business for XYZ is their web design and e-marketing, totalling 90% of their annual income. Recently, XYZ designed the website and all pamphlets for a prestigious golf estate. The website included various webcams and virtual tour features.

XYZ is also the owner of a very well-know accommodation directory and booking website. It currently has over 2000 guesthouses, guest farms and various resorts listed. Clients pay for services, such as listing on the site, web hosting and booking services, for which XYZ get commission. This site provides income for over 60% of their annual web-related income. It is because of this website that XYZ has realised that it needs seriously to consider and manage its risks.

8.4 Applying EPiRISMM at XYZ

XYZ, when first looking at EPiRISMM, was overwhelmed by the amount of activities to be performed, as well as the three levels of application. However, looking in more detail at the activities, XYZ realised that many of these activities had been performed already when the business was established in 2003. These activities included the development of the vision and mission, the identification of stakeholders, the SWOT-analysis, formulation of strategic goals, performing a gap analysis, identification of generic and corporate strategies, the evaluation and selection of the strategies and dealing with well-known financial aspects. Furthermore, according to XYZ, its structure hierarchy is "working for them", with leadership that supports it. XYZ decided to review its vision, mission and goals at this stage.

However, XYZ had not considered its values yet. XYZ articulated these values and decided on the amount of risk it is willing to accept (its risk appetite). XYZ decided that it is not willing take any large risks at a strategic level, but recognises that if it takes calculated risks, there may be possible rewards.

Next, various policies were formulated. This was a real wakeup call for XYZ, because it had not formulated any policies, whatsoever. Presented with the policy hierarchy in Figure 7-2, XYZ was again overwhelmed. It was decided that some of the policies could be combined, and that the general ICT policy would include information on information security and risk management.

Next, the various risks were identified, estimated and evaluated. This was done with the three directors of the company and consisted of brainstorming only. Various general business risks were identified. The major ICT-related risk was regarding the tourism website. If the website is down, XYZ will lose money, and it would definitely harm its corporate image. Other ICT-related risks included possible lack of new web sites to design and power outages in the region. The lack of business is considered a marketing issue and will not be considered here, while the power outages, although important, are to be handled at departmental level.

Thereafter, various risk responses were identified, and it was decided to follow a risk transference strategy for the tourism website. Discussing this, XYZ realised it already had a transference strategy in place. This was carried out by its internet-hosting provider, which guarantees 99.9% uptime and translates to only 8.5 hours of downtime a year. The hosting provider also offers backup services. In other words, it basically handles all the business continuity requirements of the tourism website. Another control that was selected at this level was the development of a security awareness program and training. It was decided to implement only the general awareness now, and when the other levels completed their activities, implement the training according to their needs. Policies were refined at this stage.

Next, it was decided to consider the monitoring activities. However, these activities are not to be performed immediately, but are reactive with constantly ongoing activities. It was decided to deal with these issues as they arise. XYZ acknowledged that it is easy to just forget about these activities or keep on putting them off until a later stage. Therefore, XYZ agreed to change its culture to one of constant learning, awareness and improvement.

XYZ also decided that it wanted to promote a culture of open communication throughout the organisation. This would ensure that all stakeholders are always kept informed and know what is expected of them.

Next, XYZ went onto the tactical level activities. For this, the various departmental heads were approached. Each of them was asked to develop a departmental mission, determine values, and other activities listed in Table 7-7, 2 a – h.

Next, the departmental managers were asked to analyse the risks that they face. This was done based on parts of detailed risk analysis discussed in Section 2.7.3. One of the largest risks identified is being late for a project due to a power failure. Others included loss of data due to hard disk failure, key staff not being available and loss of hardware, software and data due to theft. Viruses and their effects were also taken note of.

Next, the various risks and possible strategies were considered. Again, different strategies were selected for different risks. Various controls were identified, such as anti-virus programs. Business continuity plans (BCPs) must also be developed to guard against the effects of the many power failures. UPSs (Uninterrupted power supplies) were also mentioned in the BCP. XYZ also decided to write an information and ICT security policy to help guard against risks. This policy was then adopted at the strategic level and thus covers the whole organisation. Similar to the strategic level, various ongoing monitoring activities will be performed.

Because XYZ is such a small organisation, the tactical level management is the last line of management. Therefore, the last level of EPiRISMM will not be implemented.

8.5 Findings and Suggestions

The aim of this case study was to demonstrate how EPiRISMM may by used within a real-world situation. Given the nature of the case study, it was a certain test of EPiRISMM's scalability. The following observations were made:

- Most organisations have a vision and mission. This is often done in the business plan. However, more often than not, this is the last time that the vision and mission are formally considered. In the case of XYZ, employing EPiRISMM forced it to revisit its vision and mission, and thence revise it. This may prove to be valuable in the future.

- The same may be true for other activities also listed in the general activities section, such as the identification of stakeholders and the SWOT analysis.

- The activity regarding the policies may be unclear, especially on its own. Moreover, it can be seen as impossible to have all the steps in chronological order. The policies activity may be better represented in parallel with the rest of the activities in EPiRISMM.

- BCP, policies, training and ICT security plans are controls according to Table 2.2. Therefore, controls should rather be represented on a different level as "risk treatment decisions and safeguard selection".

- Another level may be added to the model, such as a level for implementation, below the operational management level, where the actual implementation takes place.

Based on the above-mentioned discussion, various improvements to the model can be identified. One example of such an improvement may include a representation of the cyclic nature of the implementation, while another may be the indication of how the policies are done in parallel with the rest of the activities.

8.6 Conclusion

This chapter examined the process of conducting a case study in an organisation with the purpose to test the proposed EPiRISMM model. This was done because the model is strongly based on theory and its real world feasibility and performance had to be tested. The results were mainly positive. It can be concluded that this model is not perfect, but can be effectively implemented. It was also found that this model can be scaled to fit organisations of various sizes. Improvements have been suggested. Once these improvements are implemented, another case study may be performed to test the model further as well as the improvements that have been made. More research may be conducted, as will be discussed in the next chapter.

Section 5: Conclusion

Chapter 9

CONCLUSION

9.1 Background

Today, enterprises will most probably come to a standstill when information resources are unavailable. Information, along with people, is considered the most important assets of an enterprise. To protect assets of an enterprise, the risks threatening these assets must be managed. Risk management practices regarding information have evolved since the introduction of computers. Back then, only physical aspects had to be considered. With the introduction of networks and the Internet, enterprises have become more dependent on the technology infrastructure and realise the importance of the right information at the right time.

Over the years, information-related risks have become increasingly difficult to manage because of the integrated nature of information. Information is used throughout all enterprise levels and departments. The need has arisen to manage information-related risks holistically. Indeed, various aspects influence the effective management of information-related risk, and a way to demonstrate these aspects will be important and relevant.

The proposed model, EPiRISMM, will reinforce and emphasise the importance of an integrated risk management philosophy. Furthermore, it will guide enterprises to align risk management practices with their vision and mission.

9.2 Summary

The following is a brief summary of each of the chapters in this dissertation. **Chapter 1** introduced the problem of misaligned risk management practices. Various problems and objectives were identified, and a model to solve the problems and reach the objectives was suggested.

Risk, and the management of risk, both from a general perspective as well as from an ICT perspective, were discussed in **Chapter 2**. Risk in general was discussed, and how it can be perceived by various parties. It was concluded that risk is the negative side of uncertainty, but that there is a positive side to it as well, called opportunity. Next, the management of risk as a concept was discussed from a general perspective, and how it can be split into risk analysis and risk management. The management of risk from an ICT perspective followed the general discussion.

Chapter 3 discussed corporate governance and highlighted why it is important. The importance of corporate governance was accentuated by discussing three well-known corporate disasters. Next, ten principles of corporate governance were listed, which were followed by a discussion on various corporate regulations and guidelines. This discussion covered regulations and guidelines such as the Treadway Commission Report, Cadbury, Turnbull, King and Sarbanes-Oxley. Chapter 3 was concluded by discussing risk management in the context of corporate governance.

In **Chapter 4** enterprise risk management was discussed. This included a general overview of what enterprise risk management (ERM) is and revisited the issue of the evolution of risk management into enterprise risk management. Next, the components of ERM were enumerated, which was followed by a presentation of various ERM frameworks. Finally, five limitations of ERM were addressed.

The importance of information was the focus of **Chapter 5**. This chapter contained a general discussion on information security, including a glance at the pillars of information security. Thereafter, it was demonstrated exactly how information came to be so important to enterprises, and how ICT-related risk management evolved from computer risk management into ICT risk management into information risk management. The problem of unaligned risk management practices between an enterprise and ICT perspective was addressed by making use of an analogy of the human body and bodily risk management. Chapter 5 was concluded by drawing parallels between the human body and enterprises, and it became clear that enterprises need to consider their risks holistically.

To address enterprise information risk holistically, a conceptual model was proposed in **Chapter 6**. First, the objective of such a model was described. Next, the development of the model resulted, and the EPiRISMM, a prism-shaped model was revealed. This model has three sides, called façades. These façades represent ICT, corporate governance and the enterprise, with information as the core of the EPiRISMM. The EPiRISMM is divided into the three levels of organisational management. Lastly, various steps were introduced that described how the prism-shaped model can be used to manage enterprise risks holistically.

The steps revealed in Chapter 6 formed the basis of discussion for **Chapter 7**. First, three regulations and guidelines were selected to fit into each of the façades of EPiRISMM, and one selected for the information core of the model. The second step was to extract activities from the selected regulations and guidelines and map them together. The last step described how the mapped activities may be applied at the three managerial levels of an enterprise.

Next, **Chapter 8** tested the theoretical model by applying it in a case study. This case study, even though it was based on elements of an anonymous working enterprise, revealed valuable insight of how the model can be applied in a real-life situation. From this practical perspective, various new ideas came to light which could be incorporated into EPiRISMM.

Finally, this chapter, Chapter 9, offers the conclusion.

9.3 Solving the Problem

The primary reason for this research endeavour was expressed in Chapter 1 as: "A major problem being experienced in the business environment today is that organisational risk cannot be managed effectively, because business and information-related risk are not congruently aligned with risk management terminology and practices." From this problem the primary objective of this study was defined, which was to develop a model to integrate risk management practices in today's business and

information environments and ultimately assist in the management of information related risks.

Various secondary objectives were identified, which assisted in the achievement of the primary objective.

The first secondary objective was to determine what the views on risk management are. This objective was achieved by performing a literature survey of various influences and recent developments regarding risk management. It was discovered that today, risk is primarily perceived as negative. Risk management, from an ICT perspective, is mainly perceived as preventing negative events from happening. However, when one moves up the organisational hierarchy, the positive side of risk, namely opportunity, becomes more evident. Therefore, it was concluded that risk and the management of risk are perceived differently in different industries, as well as at different levels of the organisational hierarchy, and thus the first secondary objective was reached satisfactorily.

The next secondary objective was to determine what factors influence information risk management in an enterprise. It was determined that ICT, corporate governance and the enterprise, as a whole, all play a pivotal role, and therefore, all these aspects must be considered when managing information-related risks. Based on the information brought forward and conclusions drawn, it can be claimed that the second secondary objective was reached.

The third secondary objective was to represent the identified influences. This objective was reached by the development of the conceptual model, EPiRISMM. EPiRISMM is in the shape of a prism, showing that information risk management is influenced by ICT, corporate governance and the enterprise as a whole. Information was represented as the core of EPiRISMM. Because EPiRISMM represents the listed influences successfully, the third secondary objective was reached successfully.

The final secondary objective was to indicate how the representation could be used to manage information-related risks holistically. This objective was reached by developing and elaborating on the three steps to implement EPiRISMM. This lead to various activities being identified that would allow information-related risks to be managed holistically. Based on the case study implemented that tested these steps, it can be claimed that the final secondary objective was reached satisfactorily.

These four secondary objectives enabled the primary objective to be accomplished by integrating ICT, corporate governance and the enterprise as a whole, thus, holistically managing information-related risks. Ultimately, this model provides any enterprise with activities to follow that will allow information risk management to be integrated within the enterprise so that it works towards the same vision of wellness for the enterprise. Thus, from the arguments above, it can be claimed that the primary objective of this dissertation, along with the secondary objectives, have been met.

9.4 Limitations of this Study

One of the biggest limitations of this study, and possibly any study consisting of a literature survey, is the information gathering process. When searching for information, one of the first problems experienced was to get enough information. Thereafter, selecting appropriate, accurate information is important and filtering out the "unnecessary" information is done; however, it is easy to overlook important information.

Another limitation of this study was the constant addition of new information in the covered areas. Because this study addressed governance, ICT and enterprise matters, it was even more difficult to keep up with the latest information in these areas.

This study is further limited by the size of EPiRISMM, which could take years to implement and require a great deal of manpower.

Finally, the scope of applicability of EPiRISMM is very large, aimed at larger enterprises. It would be extremely difficult to find such a large enterprise that would be

willing to test any model by means of a case study. However, the case study presented in this dissertation did not cover a large enterprise, but tested the scalability of EPiRISMM and included aspects of a real company. All in all, taking all of these limitations into account, the project has been successful.

9.5 Future Research Directions

Various possible directions for future research are listed below:

- The standardisation of risk and control-related terminology is desperately needed.

- A possible revision of EPiRISMM may include more focus on opportunity, the upside of risk. This may promote a more positive, risk-embracing attitude towards risk in enterprises.

- More focus may be placed on exactly how risks are managed at the various levels of an enterprise. This may include a more in-depth study of the granularity of risks, as well as how risks are perceived at the various organisational levels.

- To fortify EPiRISMM, questionnaires or interviews may be undertaken to obtain feedback from various practitioners in industry. Finally, a number of case studies may be performed and their results incorporated into the model.

9.6 Epilogue

Information is an essential asset in all organisations, but it is often taken for granted. Information requires an infrastructure to communicate it throughout an enterprise. Therefore, this infrastructure plays an important role in the management of information-related risk. Other factors to consider include corporate governance, which describes what happens at the top of an enterprise, as well as various other miscellaneous enterprise considerations. EPiRISMM can be seen as an important

guideline for enterprises to manage information-related risks. When it comes to these risks, one should be able to look at the trees while still considering the forest. It will help little if all the workers are cutting down the trees perfectly, but the leaders of the enterprise have not noticed that the workers are cutting down the wrong forest (Covey, 1989).

The proposed model, EPiRISMM, will reinforce and emphasize the importance of an integrated risk management philosophy. Furthermore, it will guide enterprises to align risk management practices with their vision and mission.

REFERENCES

Adams, J. (1995). *Risk*. London: UCL Press.

ADB. (2003). "Corporate governance principles for business enterprises." 31 May 2006, from http://www.adb.org/documents/brochures/corporate_gov/corporate_gov_principles.pdf

Agrawal, R., Findley, S., Greene, S., Huang, K., Jeddy, A., Lewis, W. W., et al. (1996). "Capital productivity: why the US leads and why it matters?" *McKinsey Quarterly, 3*, 39-48.

Ansoff, H. I. (1986). *Corporate Strategy*. London: Sidgewick & Jackson.

AS/NZS 4360:1999. (1999). "Risk management." Prepared by the joint technical committee OB/7. : Published jointly by Standards Australia and Standards New Zealand.

Bandyopadhyay, K., Mykytyn, P. P., & Mykytyn, K. (1999). "A framework for integrated risk management in information technology." *Management Decision, 37*(5), 437-445.

Barman, S. (2001). *Writing Information Security Policies*. Indianapolis: Sams Publishers.

Barton, T. L., Shenkir, W. G., & Walker, P. L. (2002). *Making Enterprise Risk Management Pay Off: How Leading Companies Implement Risk Management*. Upper Saddle River: Financial Times Prentice Hall.

Basel II. (2006). "Basel II: International convergence of capital measurement & capital standards: A revised framework - Comprehensive version." Retrieved 1 August 2006, from http://www.bis.org/publ/bcbs128.pdf

Bernstein, P. (2001). "The enlightening struggle against uncertainty." In J. Pickford (Ed.), *Mastering risk* (Vol. 1): Financial Times.

Blakley, B., McDermott, E., & Geer, D. (2001). "Information security is information risk management." Paper presented at the *Proceedings of the 2001 Workshop on New Security Paradigms* (pp 97 - 104), Cloudcroft, New Mexico.

Blomkvist, A. (1987). "Psychological aspects of values and risks." In *Risk and Society*. London: Allen & Unwin.

Booker, F. M. (2003). *An ERM framework: Developing Effective Risk Management Strategies to Protect your Organization* (White Paper, August 2003).www.grantthornton.ca/assurance/ERM%20Framework%20White%20Paper_09-12-03.pdf White Paper: Grant Thornton.

Borland Software Corporation. (2005). "Understanding and managing risk." Retrieved 5 August 2006, from http://wp.bitpipe.com/resource/org_982697212_431/Understanding_Managing_Risk-Borland_In_Network.pdf

Bornman, W. G. (2004). *Information Security Risk Management: A Holistic Framework*. Rand Afrikaans University, Johannesburg.

Borodzicz, E. P. (2005). *Risk, Crisis & Security Management*. Chichester, West Sussex, England: John Wiley & Sons.

Botterill, L., & Mazur, N. (2004). *Risk & Risk Perception: A Literature Review* (Available from http://www.rirdc.gov.au/reports/hcc/04-043.pdf).http://www.rirdc.gov.au: Astralian Rural Industries Research and Development Corporation.

Brevis, T., Vrba, M. J., & de Klerk, A. (1997). *Management Principles* (2 ed.). Kenwyn: Juta.

British Standards Institution. (1991). *Quality Vocabulary. BS4778 (Part 3 Section 3.2 = IEC 1990 50(191))* London: British Standards Institution, .

BS7799:2. (2002). *Information Security Management Systems - Specification with Guidance for Use*: BSI.

Cadbury, A. (1999). *Corporate Governance Overview*: World Bank.

Clift, S. (1999). "Information is power? Envisioning the Minnesota public Internet - Public service and community information and interaction in the public interest." (Edited transcript of the speech given by Steven Clift to the Information is Change conference in St. Paul, Minnesota on November 8, 1999) [Electronic Version]. Retrieved 17 August 2006 from http://www.publicus.net/present/public/.

CNSS. (2006). *National Information Assurance Glossary*. from http://www.cnss.gov/assets/pdf/cnssi_4009.pdf

CoCo. (1995). *Guidance on Control: Criteria of Control Board*: Canadian Institute of Chartered Accountants.

Collins Cobuild English Language Dictionary. (1987). *"Risk"*. London: Collins.

Conrow, E. H. (2003). "Effective risk management: Some keys to success." In Reston: AIAA Press.

COSO ERM. (2004a). *Enterprise Risk Management Framework: Executive Summary*: The Committee of Sponsoring Organisations of the Treadway Commission.

COSO ERM. (2004b). *Enterprise Risk Management Framework: Framework*: The Committee of Sponsoring Organisations of the Treadway Commission.

Covello, V. T., & Johnson, B. B. (1987). "The social and cultural construction of risk: Issues, methods, and case studies." In V.T. Covello & B.B. Johnson (Eds.), *The Social and Cultural Construction of Risk*. Dordrecht: D Reidel Publishing Company.

Covey, S. R. (1989). *The 7 Habits of Highly Effective People*. New York: Free Press.

Darlington, A., Grout, S., & Whitworth, J. (2001). "How safe is safe enough? An introduction to risk management." Retrieved 29 June 2005, from http://www.actuaries.ie/Events%20and%20Papers/Events%202002/2002-03-20_Risk%20Management/How_safe_is_safe_enough_March2002.pdf

DeLoach, J. (2000). *Enterprise Risk Management: Strategies for Linking Risk and Opportunity*. London: Financial Times Prentice Hall.

Douglas, M. (1990). "Risk as a forensic resource." *Daedalus, 19*(4), 1-17.

Dupree, M. (1989). *Leadership is an Art*. New York: Dell Publishing.

Eloff, J. H. P., Labuschagne, L., & Badenhorst, K. P. (1993). "A comparative framework for risk analysis methods." *Computers & Security, 12*(6), 597-603.

Encarta Reference Library. (2005a). Board of Directors.

Encarta Reference Library. (2005b). CEO.

Encarta Reference Library. (2005c). Chance.

Encarta Reference Library. (2005d). Uncertainty.

Fiksel, J., Low, J., & Thomas, J. (2004). "Linking sustainability to shareholder value." Retrieved 4 February 2005, from http://www.awma.org/em/pdfs/2004/6/fiksel.pdf

Friedman, K. (1987). "The study of risk in social systems: an anthropological perspective." In L. Sjöberg (Ed.), *Risk and Society*. London: Allen & Unwin.

Frosdick, S. (1997). "The techniques of risk analysis are insufficient in themselves." *Disaster Prevention and Management, 6*(3), 165-177.

Frosdick, S., & Odell, A. (1996). "Practical management of programme risk: the case of the national strategy for police information systems for England and Wales." *Information Management & Computer Security, 4*(5), 24-33.

Garratt, B. (2003). *Thin on Top: Why Corporate Governance Matters and How to Measure and Improve Board Performance*. London: Nicholas Brealey Publishing.

Garvin, T. (2001). "Analytical paradigms: the epistemological distances between scientists, policy makers, and the public." *Risk Analysis, 21*(3), 443-455.

Gerber, M., & von Solms, R. (2001). "From risk analysis to security requirements." *Computers & Security, 20*(7), 577-584.

Gerber, M., & von Solms, R. (2005). "Management of risk in the information age." *Computers & Security, 24*(1), 16-30.

Graubard, S. R. (1990). Preface to the issue "Risk". *Daedalus, 119*(4), v-vi.

Greenbury. (1995). *Directors' Renumeration: Report of a Study Group Chaired by Sir Richard Greenbury* London: Study Group on Directors' Renumeration.

GTAG 1. (2005). "Information Technology Controls". Retrieved 02 April 2007, from http://www.theiia.org/guidance/technology/gtag/gtag1

Halliday, S., Badenhorst, K., & von Solms, R. (1996). "A business approach to effective information technology risk analysis and management." *Information Management & Computer Security, 4*(1), 19-31.

Hample. (1998). *UK Hample Committee Report on Corporate Governance.* London: Gee Publishing.

Harding, R. (1998). *Environmental Decision-Making: The Roles of Scientists, Engineers and the Public.* Sydney: The Federation Press.

Hare, C. (2004). "It is all about control." In H. F. Tipton & M. Krause (Eds.), *Information Security Management Handbook*. London, New York, Washington D.C., Boca Raton: Auerbach Publications.

Heeks, R., & Duncombe, R. (2001). "A handbook for enterprise support agencies in developing countries." Retrieved 10 August 2006, from http://www.man.ac.uk/idpm/ictsme.htm

Henry, K. (2004). "Risk management and analysis." In H. F. Tipton & M. Krause (Eds.), *Information Security Management Handbook* (5 ed.). London, New York, Washington D.C., Boca Raton: Auerbach Publications.

Humprheys, E. J., Moses, R. H., & Plate, E. A. (1998). *Guide to BS7799 Risk Assessment and Management*: British Standards Institution.

Hunt, B. (2001). "Issue of the moment: the rise and rise of risk management." In J. Pickford (Ed.), *Mastering risk* (Vol. 1, pp. 289-294): Financial Times.

Hwang, J. D. (2002). "Information resources management: New era, new rules." *IT Professional, 4*(6).

InfoSecPedia. (2006). "CIA triad." Retrieved 10 August 2006, from http://www.infosecpedia.org/pedia/index.php/CIA_triad

ISO/IEC 13335-1. (2004). *Information Technology - Security Techniques - Management of Information and Communications Technology Security Part 1: Concepts and Models for Information and Communications Technology Security Management* (Tech. Rep.): ISO/IEC.

ISO/IEC 17799. (2005). *Information Technology - Security Techniques - Code of Practice for Information Security Management* (Tech. Rep.): ISO/IEC.

ISO/IEC 27001. (2005). *Information Technology – Security Techniques – Information Security Management Systems – Requirements.* ISO/IEC.

ISO/IEC TR 13335-3. (1998). *Information Technology - Guidelines for the Management of IT Security Part 3: Techniques for the Management of IT Security* (Tech. Rep.):ISO/IEC.

IT Governance Institute. (2000). *Cobit 3rd Edition - Executive Summary*: Information Systems Audit and Control Foundation.

ITGI. (2003). *Board Briefing on IT Governance* (2nd ed.).Available from http://isaca.org/content/contentgroups/itgi3/resources1/board_briefing_on_IT_governance/26904_Board_Briefing_final.pdf Rolling Meadows, IL, USA: The IT Governance Institute.

IWS. (2005). "Computer and Information Security." Available from http://www.iwar.org.uk/comsec/

Keen, P. G. W. (1991). *Shaping the Future: Business Design through Information Technology*. Cambridge: Harvard Business School Press.

Ketz, J. E. (2003). *Hidden Financial Risk: Understanding Off-Balance Sheet Accounting.* Hoboken: John Wiley & Sons, Inc.

King I. (1994). *The King I Report on Corporate Governance in South Africa.* Available from http://www.iodsa.co.za/IoD: The Institute of Directors.

King II. (2002). *The King II Report on Corporate Governance in South Africa.* Available from http://www.iodsa.co.za/IoD: The Institute of Directors.

Kirkwood, A. S. (1994). "Why do we worry when scientists say there is no risk?" *Disaster Prevention and Management, 3*(2), 15-22.

Klein, M. (2001). "The rise and fall of LeisureNet." Retrieved 05 July 2006, from http://209.117.96.104/articles/01_01leisurenet.pdf

Kroon, J. (1996). *General Management* (2 ed.). Pretoria: Kagiso Tertiary.

Lam, J. (2000). "Enterprise-wide risk management and the role of the chief risk officer" [Electronic Version]. *ERisk*. Retrieved 11 July 2006 from http://www.erisk.com/Learning/Research/011_lamriskoff.pdf.

Leitch, M. (2005). "Why the COSO frameworks need improvement" [Electronic Version]. *IRMI - Expert Commentary*. Retrieved 14 November 2005 from http://www.irmi.com/expert/articles/2005/Leitch04.aspx.

Lichtenberg, G. C. (1742-1799). Classical work - German physicist, philosopher. "Notebook D," aph. 5, Aphorisms (written 1765-1799), trans. by R.J. Hollingdale (1990).).

Marchewka, J. T. (2003). *Information Technology Project Management: Providing Measurable Organizational Value*. New York: John Wiley and Sons, Inc.

Merkofer, M. W. (1987). *Decision Science and Social Risk Management*. Dordecht: D Reidel Publishing Company.

Moberg, D., & Romar, E. (2003). *WorldCom*. Retrieved 04 July 2006, from http://www.scu.edu/ethics/practicing/focusareas/worldcom.cfm.

Moses, R. H. (1992). "Risk analysis and management." In K. M. Jackson & J. Hruska (Eds.), *Computer Security Reference Book*. Oxford: Buttorworth-Heinemann Ltd.

Naidoo, R. (2002). *CorporateGgovernance*. Cape Town: Double Storey Books.

NIST SP 800-30. (2001). *NIST Special Publication 800-30: Risk Management Guide for Information Technology Systems*: National Institute for Standards and Technology.

Ozier, W. (2004). "Risk analysis and assessment." In H. F. Tipton & M. Krause (Eds.), *Information Security Management Handbook*. London, New York, Washington D.C., Boca Raton: CRC Press LLC.

Phillips, B., & D'Orso, M. (1999). *Body for Life*. New York: Harper Collins Publishers.

Reynolds, R. (2003). "How effective is your risk culture?" *PWC: Insurance Digest*, 16-19. Available from http://www.pwcglobal.com/images/gx/eng/fs/insu/americas_ins_digest_feb2003.pdf

Rossouw, D., le Roux, S., & Groenewald, D. (2003). *Strategic Management: A South African Perspective*. Cape Town: ABC Press.

Royal Society. (1983). *Risk Assessment* (Report of a Royal Society study group). London.

Royal Society. (1992). *Risk: Analysis, Perception and Management* (Report of a Royal Society study group). London.

Scarff, F., Carthy, A., & Charette, R. (1993). *Introduction to the Management of Risk*. Norwich: HMSO.

Schultz, B. R. (2004). "Evaluating the security posture of an information technology environment: The challenges of balancing risk, cost, and frequency of evaluating safeguards." In H. F. Tipton & M. Krause (Eds.), *Information Security Management Handbook*. London, New York, Washington D.C., Boca Raton: Auerbach Publications.

Schwalbe, K. (2002). *Information Technology Project Management* (2 ed.): Thompson Learning.

Seeley, R. R., Stephens, T. D., & Tate, P. (1989). *Anatomy and Physiology*. St Louis, Toronto, Boston, Los Altos: Times Mirror / Mosby College Publishing.

Simister, T. (2000). "Risk management: the need to set standards". *Balance Sheet, 8*(4), 9-10.

Slovic, P. (1999). "Trust, emotion, sex, politics, and science: Surveying the risk-assessment battlefield." *Risk Analysis, 19*(4), 689-701.

SOX. (2002). *The Sarbanes-Oxley Act*. Senate and House of Representatives of the United States of America

Spangler, M. B. (1984). "Policy issues related to worst-case risk analyses and the establishment of acceptable standards of deminimising risk." In V.T. Covello, L.B. Lave, A. Moghissi & V.R.R. Uppuluri (Eds.), *Uncertainty in Risk Assessment, Risk Management, and Decision Making*. New York: Plenum Press.

Supportinet. (2006). Combined code. Retrieved 04 July 2006, from http://www.combinedcode.com

Sutherland, J., & Canwell, D. (2004). *Key Concepts in Strategic Management*. New York, Hampshire: Palgrave MacMillan.

Tchankova, L. (2002). "Risk identification - basic stage in risk management." *Environmental Management and Health, 13*(3), 290-297.

Tipton, H. F. (2004). "Types of information security controls." In H. F. Tipton & M. Krause (Eds.), *Information Security Management Handbook*. London, New York, Washington D.C., Boca Raton: Auerbach Publications.

Treasury Board of Canada. (2001). *Integrated Risk Management Framework*.

Tricker, R. I. (1984). *Gorporate Governance*. Aldershot: Gower Publishing Company.

Turn, R. (1986). "Security and privacy requirements in computing." Paper presented at the proceedings of 1986 Fall Joint Computer Conference on fall joint computer computer conference.

Turnbull. (1999). *Internal control - Guidance for Directors on the Combined Code*.

Van der Merwe, J., Appleton, R., Mahony, D., & Koen, M. (1995). *Corporate Business Administration*. Cape Town: Juta.

Vinten, G. (2001). "Corporate Governance and the Sons of Cadbury." *Corporate Governance, 1*(4), 4-8.

Von Solms, R. (1998). "Information security management (1): Why information security is so important." *Information Management & Computer Security, 6*(4), 174-177.

Whitman, M. E. (2003). "Enemy at the gates: Threats to information security." *Communications of the ACM, 46*(8), 91-95.

Whitman, M. E., & Mattord, H. J. (2003). *Principles of Information Security*. Boston: Thomson Course Technology.

Wikipedia. (2006a). Chairperson. Retrieved 06 June 2006, from http://en.wikipedia.org/wiki/Chairman

Wikipedia. (2006b). COBIT. Retrieved 23 October 2006, from http://en.wikipedia.org/wiki/CobiT

Wikipedia. (2006c). Data integrity. Retrieved 06 June 2006, from http://en.wikipedia.org/wiki/data_integrity

Wikipedia. (2006d). Enron. from http://en.wikipedia.org/wiki/enron

Wikipedia. (2006e). Information. Retrieved 10 August 2006, from www.wikipedia.org/wiki/information

Wikipedia. (2006f). Information security. Retrieved 06 June 2006, from http://en.wikipedia.org/wiki/Information_security

Wikipedia. (2006g). Information technology infrastructure library. Retrieved 23 October 2006, from http://en.wikipedia.org/w/index.php?title=ITIL&redirect=no

Wikipedia. (2006h). Shareholder. Retrieved 06 June 2006, from http://en.wikipedia.org/wiki/Shareholder

Williams, C. A., Smith, C. A., & Young, P. C. (1998). *Risk Management and Insurance*. New York: McGraw Hill

Wixley, T., & Everingham, G. (2002). *What You Must Know about Corporate Governance*: Cape Town: Siber Ink.

Paper published in Computer Fraud and Security, December 2006

'Towards Enterprise Information Risk Management'

Towards Enterprise Information Risk Management

Neil Lategan, Centre for Information Security Studies, Nelson Mandela Metropolitan University, South Africa, nlategan@gmail.com

Rossouw von Solms, Centre for Information Security Studies, Nelson Mandela Metropolitan University, South Africa, rossouw.vonsolms@nmmu.ac.za

ABSTRACT

This paper addresses the concept of integrated risk management by making use of an analogy of the human body. Firstly, this paper argues that, for a human to enjoy a quality life, a body that is functioning effectively is required. To accomplish this, the risks that a human body faces must be managed properly. Next, the similarities between a human body and an enterprise are highlighted, where-after it is reasoned that an enterprise needs to adopt similar risk management practices to be effective. Ultimately, this paper reinforces the importance of the adoption of integrated risk management practices throughout the enterprise.

KEYWORDS

Risk Management, Integrated Risk Management, Information Risk Management, Enterprise Information Risk Management

Introduction

The business world has changed radically over the last few decades. Information and information technology have become cores to most businesses. Few enterprises today can claim that they are not totally dependent on information and its related technologies to drive their business processes and to gain, or maintain, a competitive edge. Information and its related technologies have seamlessly become part of almost all business activities.

Unfortunately, along with all the new opportunities that IT has brought, it has also given rise to many new risks. These risks, along with others, need managing to ensure that an enterprise will keep functioning effectively. That IT has become completely integrated into business is giving rise to a new paradigm as far as enterprise risk management is concerned. Therefore, an all-inclusive approach to it is needed.

This paper will address the topic of an integrated management approach for all enterprise information risks. The objective of this paper is twofold: firstly, to indicate the dissimilar natures of information and organizational risk management practices. The second is to reinforce the importance of the development of an enterprise-wide risk management strategy.

In order to reach these objectives, this paper makes use of the analogy of comparing a modern enterprise to the human body and relates this to enterprises and their risk management practices. Following the analogy, various issues concerning enterprise risk management are identified and discussed. Lastly, a conclusion is offered.

Risk management to ensure a quality lifestyle

"Your body is the epicentre of your universe. You go nowhere without it. It is truly the temple of your mind and your soul. If it is sagging, softening, and aging rapidly, other aspects of your life will soon follow suit" (Phillips & D'Orso, 1999).

It can be argued that the human body is the 'vehicle' for individuals through life. All humans want to experience a quality life, and in order to live it, individuals need to have properly functioning vehicles for their journey.

However, what a 'quality life' entails does, of course, differ from person to person (Figure 1A). Stephen Covey (1989) identified various centres in the lives of individuals. Some of these include family, money, pleasure, enmity, friendship, religious faith and self-centredness. For example, one person enjoys a quality life if he/she can perform exceptionally well on the sport field, and his/her whole life revolves around sport. For another person, a quality lifestyle could mean having a lot of money, and every action contributes to financial empire building. Yet another person's life could revolve around their family. Nonetheless, all human beings desire a quality life.

Normally, no matter what a person deems as a quality lifestyle, everyone requires a healthy body to experience it. A healthy, functioning body contains numerous systems that constitute it. These systems function and interact seamlessly and depend, to a large extent, on each other. As indicated in Figure 1 B & C, these systems holistically contribute to a quality lifestyle. Examples of these include the cardiovascular, digestive, nervous and muscular systems. Some of these have various sub-systems, for example, cardiovascular, which consists of a heart, arteries and veins, which are considered systems in their own right. All systems in the human body are integrated,

interdependent, in synergy, and altogether more than the sum of their parts (Figure 1 C). An example of such integration and interdependence are the cardiovascular and respiratory systems, which together form the cardio-respiratory system.

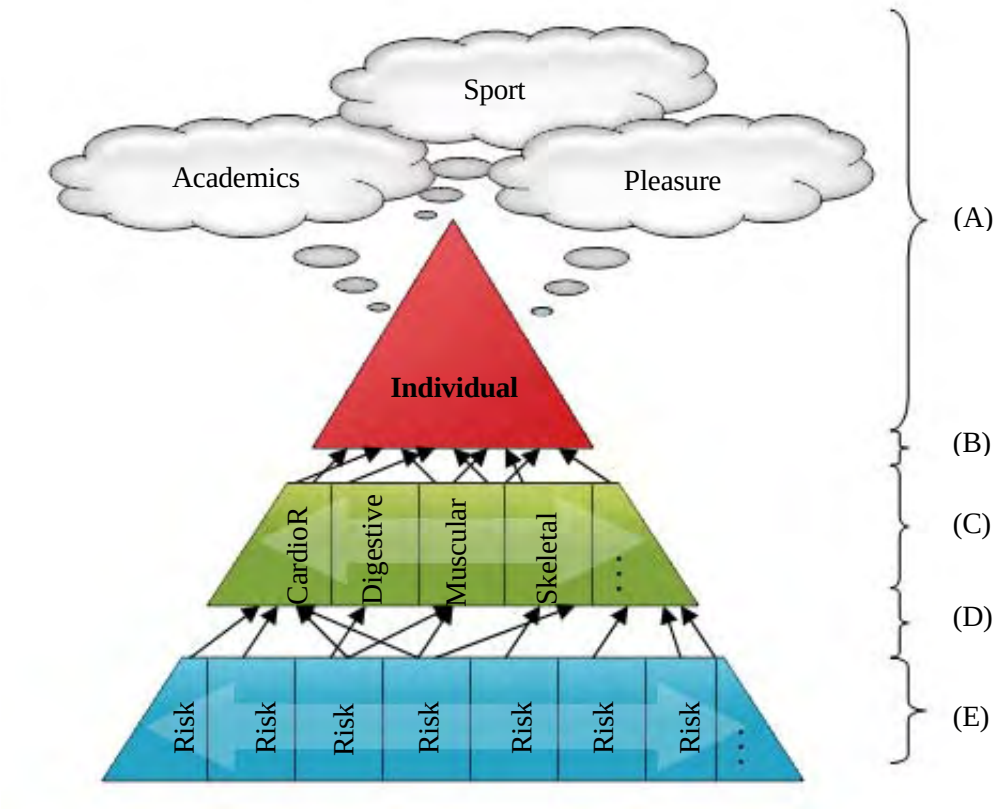


Figure 1: Bodily Risk Management

This system's function is to ensure that the various organs and limbs receive the required amount of oxygen and consists of the heart, the lungs, the arteries, the veins and the blood. The lungs extract oxygen from the air and place it in the blood. The heart then pumps the blood through the arteries and veins to the various parts of the body. Notwithstanding, there is a great deal more to the system, such as transporting nutrients, waste products and hormones throughout the body and regulating blood pH and body temperature (Seeley, Stephens & Tate, 1989). So, if the cardio-respiratory system's

effective functioning is of the utmost importance to the well-being of the human body, so it is also to the quality of life.

Risks, like injury and illness, could threaten all the systems or affect only one. However, if one system fails, others will soon follow suit. Eventually, the quality life of the individual, whatever it may be, is at jeopardy.

To ensure the proper working of the cardio-respiratory system, and ultimately ensuring a quality lifestyle, these risks should be managed. Typically, risk management activities include performing cardiovascular exercise, such as running or aerobics. This will give the whole cardio-respiratory system exercise and improve oxygen supply to the entire body as a result. Another risk management activity may be eating the right foods, such as fresh fruit and vegetables, and avoiding fatty foods. This might help to prevent cancer and will certainly assist in controlling high, unhealthy cholesterol levels. On the contrary, there are activities that negatively influence the human body. An example of such a harmful activity that should be avoided is smoking, which may cause lung cancer. Furthermore, some risks fall outside the control of the individual, for example, hereditary disease. In addition, regular medical checkups are advised to monitor and evaluate the overall health situation.

It is important to note that all of these factors are interdependent. Exercising alone will not normally ensure a healthy heart, and it is possible one could have a healthy heart but weak lungs, for example, which is not conducive to a healthy body or a quality lifestyle. Furthermore, some risks affect more than one organ or system, but some risk management practices can control more than one risk (see Figure 1 D & E). For

example, a healthy diet will positively affect the digestive system, the cardiovascular system, the skeletal system, and most other systems in the human body.

If an individual falls ill, normally some risk materialized and influenced one or other of the bodily systems. Although only one system may be malfunctioning, because of the ailment, the complete body will be influenced, and the individual will not enjoy a quality life whilst ill. Normally, in situations like this, the individual might visit a medical doctor who will examine the individual, diagnose the problem and prescribe some treatment. This should cure the ailment, ensure that the influenced system functions properly again and restore the health of the individual to again enjoy life.

Thus, it can be concluded that:

- Quality of life depends on a healthy body;
- A healthy body depends on a set of properly functioning systems;
- These systems are all interdependent;
- Various risks threaten every system;
- If one of the risks materializes, it will have a negative effect on at least one of the systems with the result that the whole body will suffer and quality of life will be influenced;
- Risks are managed in a holistic way through exercise, healthy eating, not smoking, etc. The eventual goal is to ensure a healthy body that will enable a quality life;

- The aim of risk management is not to focus separately on individual systems, but rather to determine what is required to ensure a quality life and to ensure that a holistic, all-inclusive risk treatment plan is introduced to guarantee a healthy body and mind that, in turn, depends on properly functioning systems.

Risk management from an enterprise perspective

The previous section discussed risk management as an integral exercise to ensure a quality lifestyle for a human being. It can be argued that an enterprise has a 'life', and that this enterprise also wants to maximize the quality of its lifestyle. This refers to its mission and vision (Figure 2A). Enterprises can have different missions and visions, and a quality lifestyle can mean different things to different enterprises. Examples of these include profits, good working conditions, creating jobs, etc.

Similar to the human body, an enterprise consists of various systems. These departments, processes and systems operate interdependently, but most of them are linked to and dependent on IT systems. However, there are various risks threatening this synergy of systems, and these therefore also threaten the mission and vision of an enterprise. These should be properly managed in a holistic and all inclusive manner (Figure 2). The rest of this section will compare an enterprise's 'life' and risk management to that of human beings.

It has been said that information is the lifeblood of an enterprise (Halliday, Badenhorst & von Solms, 1996), with the heart and veins being the information and communication technology (ICT). Similar to the cardio-respiratory system, ICT systems are totally integrated and interdependent on the rest of the enterprise systems. The heart of the

enterprise, the ICT department, pumps information (the blood) to and from processes and activities through the networks and communication channels, which can be considered the veins and arteries of the enterprise. As mentioned before, the digestive system absorbs nutrients from food and then transports them via the bloodstream. Similarly, various enterprise departments gather information that is then processed and transported horizontally and vertically through an enterprise. If information arrives at the right place at the right time, informed decisions can be made, and business processes can function. If this happens successfully, the enterprise is moving closer to reaching its mission and vision.

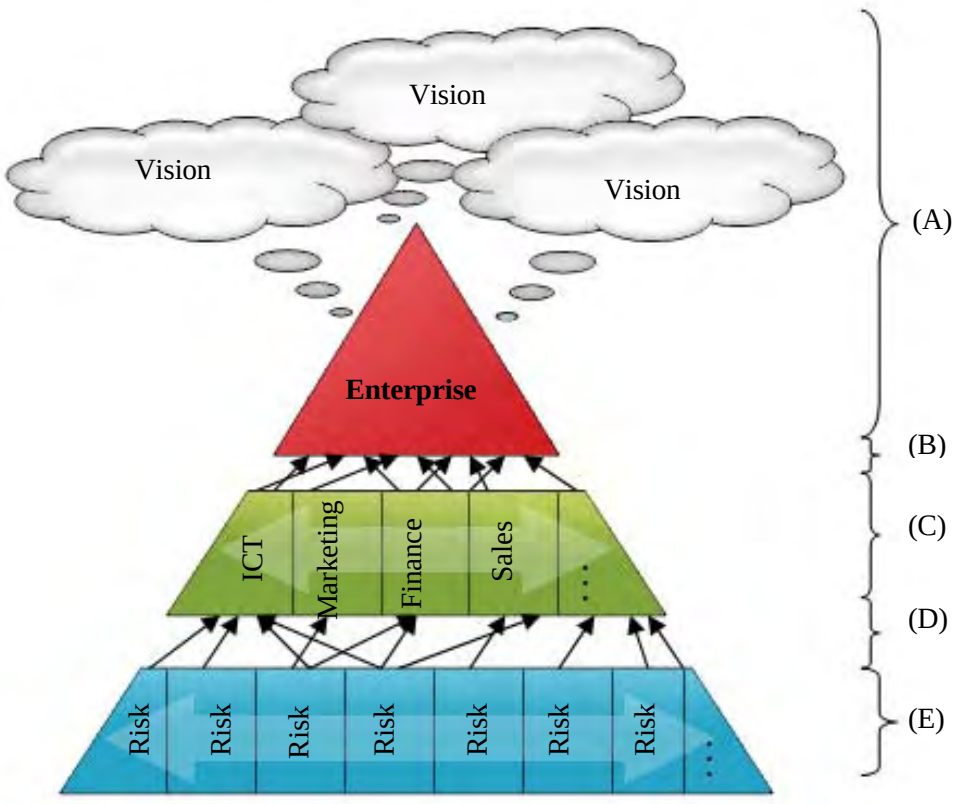


Figure 2: Risk management from an enterprise perspective

If something goes wrong with the heart, or if the veins are clogged-up with cholesterol, supplies of nutrients and oxygen will not reach the dependent systems effectively. If the enterprise's 'heart', the ICT department, is not functioning properly, information cannot be 'pumped' to the business systems where needed. Some processes that are totally dependent on information, might event cease to function. Nonetheless, if the heart is weak, it does not necessarily mean that the rest of the system will not function, but it will not function optimally. From an enterprise's perspective, if the ICT is down, the rest of the enterprise will also be impacted upon. The magnitude of the impact will rest on how dependent the enterprise is on ICT and will change from enterprise to enterprise.

A human being, who wants to ensure that his/her cardio-respiratory system functions optimally, has to continually manage their body well and even undergo a change of lifestyle, if necessary. In an enterprise, risks need to be managed as well. All human resources, from the Board right through to the floor, need to adopt such an enterprise-wide risk management culture and take responsibility for risk management (King II, 2002).

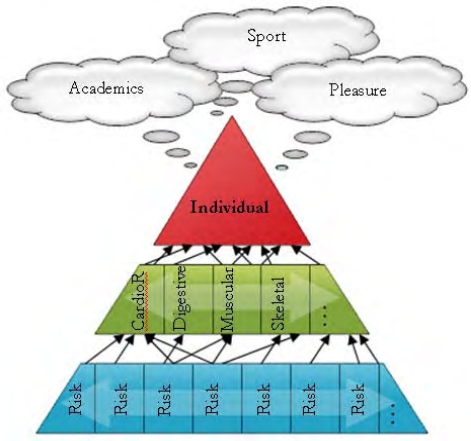
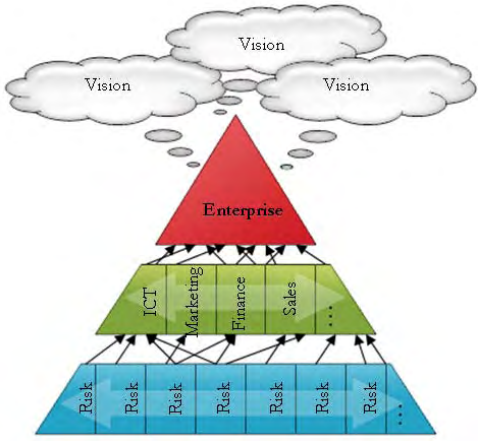
In an enterprise, some risks threaten more than one system or department. Some risk measures that are taken may help cater for various risks and have an impact on more than one department (Figure 2 D). Additionally, risk management in an enterprise is not a once-off activity, but an ongoing process - a change in lifestyle. To establish and maintain such a process, discipline and dedication are required and these call for the corporate culture to adapt accordingly. Furthermore, an all-inclusive approach to risk management must take place in all enterprise departments and systems, not just a select few.

If a human being falls sick, he/she seeks medical attention from a doctor, whereas in an enterprise this is done by a risk manager. Blakley, McDermott and Geer (2001) argue that information risk should be managed by professionals with similar characteristics as physicians. These include (Blakley *et al.*, 2001):

- Professional and specialized education;
- License to practice that can be revoked;
- Ethical obligation that they will handle their patients and their personal information with care;
- Professional obligation to handle and control adverse conditions by means of prescription;
- Professional obligation to report on any relative and important information to the right authorities.

Table 1 provides a summary of all comparative arguments for qualities of life for both a human being and an enterprise.

Table 1: A Comparison of Risk Management from and Human and Enterprise Perspective

The human body	**The enterprise**
	
Quality life is ultimately the vision of the individual person.	A quality 'life' is ultimately the vision of any enterprise.
This quality life means different things to different people: it can be fame, money, sporting achievements, etc.	The quality life means different things to different enterprises, examples are financial success, creating jobs, being socially responsible, etc.
The quality life depends on the various systems of the body functioning effectively.	The quality lifestyle of the organization depends on its various departments, systems and processes functioning effectively.
The function of the cardio-respiratory system is to make sure oxygen and other important nutrients get to where they are needed at the right time in the right quantity for individual systems to function.	The function of ICT is to make sure information arrives at the right time in the right format where it is needed for individual systems to function.
If the cardio-respiratory system and other systems function effectively, the individual <u>can</u> enjoy a quality life.	If the ICT and other systems function effectively, the enterprise <u>can</u> have a quality 'life'.
All systems, including the cardio-respiratory system, have risks that threaten it and ultimately threaten the well-being of the individual person.	All systems, including the ICT, have risks that threaten its well-being and ultimately threaten the well-being of the enterprise.
These risks need to be managed.	These risks need to be managed.
A doctor helps the individual manage his/her	A risk manager helps the enterprise manage its

health risks, while it is ultimately the responsibility of the individual.	risks, while it is ultimately the responsibility of everyone in the enterprise.
If all health risks are properly managed, the chances of a healthy working body and mind are increased, which means a quality life is possible.	If all business risks are properly managed the chances of a 'healthy', effective company is increased and a quality 'life' for the company is possible.
The risks associated with the cardio-respiratory system are not managed independently of the risks of other bodily systems.	The risks associated with ICT should not be managed independently of the risks of other systems.
The risk management process for the cardio-respiratory system is integral to the overall objective of the human being and, therefore, all risk management processes need to be integrated to ensure the objectives are reached.	The risk management process for the ICT system is integral to the overall objective of the enterprise and, therefore, all risk management processes need to be integrated to ensure the overall enterprise objectives are reached.

Today, enterprises must ensure that risks are managed holistically and that ICT-related risk terminology and practices are congruently aligned with those of the enterprise. The business environment and information technology are bound together by information (Eloff, Labuschagne & Badenhorst, 1993). For this reason, it is imperative that risk management is synergized in the business, IT and information worlds. A thorough, all-inclusive risk analysis exercise needs to be conducted in business *and* supporting environments in order to develop an effective internal control system. Such an internal control system should reduce the exposure of risk and aid the safeguarding of assets (Cadbury, 1999). Indeed, in today's so-called information age, where business processes integrate the business and ICT environments, it is imperative that a unary internal control system be established, based on a holistic risk management exercise.

Conclusion

For a human being to enjoy a quality live, a healthy body is a pre-requisite. A healthy body cannot be achieved with a quick-fix pill; rather an all-inclusive, integrated risk management approach is required. The resultant healthy body will enable an associated healthy lifestyle, and ultimately a quality life can be enjoyed. Similarly, ICT is, to a large extent, an enabler for a quality lifestyle of an enterprise and ultimately contributes towards the mission and vision of the enterprise. For the same reasons mentioned above, an all-inclusive, integrated, enterprise-wide risk management approach needs to be adopted. ICT cannot be seen any longer as a freestanding component as far as risk management is concerned. It should form part of a holistic, integrated enterprise risk management exercise that should ensure that the whole enterprise is 'healthy' to ensure maximum probability that the vision and mission can be met.

References

Blakley, B., McDermott, E. & Geer, D. (2001). *Information security is information risk management.* In *Proceedings of the 2001 workshop on new security paradigms* (pp 97 - 104), Cloudcroft, New Mexico. ACM Press

Cadbury, S. A. (1999). *Corporate Governance Overview*: World Bank.

Covey, S. R. (1989). *The 7 habits of highly effective people*. New York: Free Press.

Eloff, J. H. P., Labuschagne, L. & Badenhorst, K. P. (1993). A comparative framework for risk analysis methods. *Computers & Security, 12*(6), 597-603.

Halliday, S., Badenhorst, K. & von Solms, R. (1996). A business approach to effective information technology risk analysis and management. *Information Management & Computer Security, 4*(1), 19-31.

King II. (2002). *The King II Report*: The Institute of Directors.

Phillips, B. & D'Orso, M. (1999). *Body for Life*. New York: Harper Collins Publishers.

Seeley, R. R., Stephens, T. D. & Tate, P. (1989). *Anatomy and Physiology*. St Louis, Toronto, Boston, Los Altos: Times Mirror / Mosby College Publishing.