Towards a Framework for Corporate Information Governance

by

Lynette May Mears
Towards a Framework for Corporate Information Governance

by

Lynette May Mears

Dissertation

submitted in fulfillment
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

Promoter: Prof. Rossouw von Solms

January 2006
Declaration

I, Lynette May Mears, 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 fulfillment of the requirements for an equivalent or higher qualification at any other recognised education institution.

Lynette May Mears
Abstract

Information is a critical asset without which an organisation could not survive. The adequate and effective governance of this asset is an essential function and is the direct responsibility of the board and senior management. The board and senior management have a responsibility to maintain the financial and material health of their enterprise and this includes setting the proper direction and governance of the information asset. Many organisations have, over the past few years, suffered severe losses and failures due to the inadequate governance and protection of this valuable asset. The reasons for the lack of corporate information governance need to be examined. The board and senior management need to direct and control their organisations effectively, with the appropriate delegation of responsibilities, to reduce the possibility of suffering similar losses and/or failures. The contribution made by this study is illustrated in the designing of a framework and activity plans to facilitate the board in practically implementing an improved corporate information governance process.
Acknowledgments

My sincerest gratitude to the following people:

• My promoter, Professor Rossouw von Solms for his support, patience and guidance.

• The National Research Foundation for the funding they provided.

• My husband, Harry, for his help, encouragement and belief in me.

• And above all, to my God.
Contents

Declaration i
Abstract iii
Acknowledgments v

I Introduction 1

1 Introduction 3
  1.1 Background ................................................. 3
  1.2 Area of Study .............................................. 4
  1.3 Problem Statement ......................................... 5
  1.4 Objectives .................................................. 6
    1.4.1 The Primary Objective .................................. 6
    1.4.2 Secondary Objective ..................................... 6
  1.5 Methodology ............................................... 7

II Background 11

2 Information and Corporate Governance 13
  2.1 Introduction ............................................... 14
  2.2 Some Recent Company Failures/Losses and the Causes ...... 15
  2.3 Relationship between Organisational Structure and Information 16
    2.3.1 Organisational Structure ............................... 17
    2.3.2 Information ............................................ 17
    2.3.3 The Utilization of Data and Information within the Organisational Structure .................. 18
2.4 Role of Information Management ........................................ 20
2.5 Role of Information Governance ....................................... 21
2.6 Corporate “Sins” .......................................................... 23
2.7 Corporate Governance ..................................................... 23
  2.7.1 Corporate Governance History ................................... 24
  2.7.2 What is Corporate Governance and what is its importance? .................................................. 24
  2.7.3 Functions of Corporate Governance ......................... 25
  2.7.4 The Roles and Responsibilities of the Board ............ 27
  2.7.5 The Responsibility for Information Governance ....... 29
2.8 Conclusion ................................................................. 30

3 Corporate Information Governance ........................................ 33
  3.1 Introduction ............................................................... 34
  3.2 Corporate Information Governance Defined .................. 34
  3.3 Components of Corporate Information Governance .......... 35
    3.3.1 Why should information technology be considered a governance issue? ....................................... 36
    3.3.2 Why should information security be considered a governance issue? ......................................... 37
    3.3.3 How do the components of information technology and information security governance combine within corporate information governance? ........................................ 40
  3.4 Structuring Corporate Information Governance Responsibilities ........................................ 41
  3.5 Conclusion ................................................................. 46

4 The Governance of Information Technology ............................. 47
  4.1 Introduction ............................................................... 48
  4.2 Aspects of Information Technology ................................. 48
    4.2.1 The Definition of Information Technology ............. 49
    4.2.2 The Evolution of Information Technology ............. 49
    4.2.3 The Purpose of Information Technology ............... 50
    4.2.4 The Expectations for Information Technology ....... 51
  4.3 Why is Information Technology Important? ..................... 52
    4.3.1 IT is critical to the organisation .......................... 52
    4.3.2 IT is strategic to the organisation ....................... 53
## CONTENTS

6.2 Core Aspects and Fundamental Issues .............................................. 94
6.3 Questions and Answers ................................................................. 98
  6.3.1 Core Aspect 1: Strategic Planning ........................................ 98
  6.3.2 Core Aspect 2: Value Delivery ............................................. 102
  6.3.3 Core Aspect 3: Risk Management ........................................ 103
  6.3.4 Core Aspect 4: Resource Management ................................... 105
6.4 Conclusion .................................................................................. 110

7 A Corporate Responsibility Matrix .................................................. 113
  7.1 Introduction ............................................................................. 114
  7.2 Criteria for the Development of a Corporate Responsibility Matrix ............................................. 115
  7.3 Process of Corporate Information Governance ............................................. 116
  7.4 Components of the Matrix ......................................................... 117
  7.5 The Corporate Responsibility Matrix .......................................... 118
    7.5.1 Modular Activity Plans ..................................................... 120
    7.5.2 A. Directing Components .................................................. 122
    7.5.3 B. Controlling Components .............................................. 134
    7.5.4 C. Responsibility Components .......................................... 136
  7.6 Benefits of Implementing the Matrix ........................................... 137
  7.7 Conclusion ............................................................................... 139

IV Conclusion ...................................................................................... 141

8 Conclusion .......................................................................................... 143
  8.1 Introduction ............................................................................... 144
  8.2 Summary .................................................................................... 144
  8.3 The Problem and its Solution ...................................................... 147
  8.4 Perceived Achievements of this Project ........................................ 149
  8.5 Perceived Limitations of this Project ........................................... 149
  8.6 Further Research ....................................................................... 149
  8.7 Conclusion ............................................................................... 150

References ............................................................................................ 151
List of Figures

1.1 Outline of chapters in dissertation ........................................ 9
2.1 The Traditional Managerial Hierarchy ...................................... 17
2.2 The Five Stages in the Development of Strategic Information Management .............................................................. 21
2.3 Corporate Governance, its Roles and Responsibilities .............. 29
3.1 Corporate Information Governance and its Components ........... 41
3.2 Corporate Information Governance Structure .......................... 45
7.1 Process of Corporate Information Governance ............................ 117
7.2 Corporate Responsibility Matrix .......................................... 119
7.3 Modular Activity Plan ..................................................... 121
7.4 Modular Activity Plan for Strategic Planning ............................ 124
7.5 Modular Activity Plan for Value Delivery ................................. 127
7.6 Modular Activity Plan for Risk Management ............................ 130
7.7 Modular Activity Plan for Resource Management ...................... 133
List of Tables

5.1 Impact of Recent Information Security Legislation . . . . . . . 75

6.1 Tabular Summary of Core Aspects and Fundamental Issues . . 111
Part I

Introduction
Chapter 1

Introduction

1.1 Background

Corporate governance is generally about holding the balance between economic and social goals and between individual and communal goals (World Bank, 1999). Corporate governance is about encouraging the efficient use of the resources of the organisation and being accountable for their stewardship. Good corporate governance provides protection in various areas. The absence of this protection and difficulties in monitoring could mean that capital providers, who lack control over the organisation, will find it both risky and costly to protect themselves from the opportunistic behaviour of managers or controlling shareholders (World Bank, 1999).

The lack of internal controls within corporate financial reporting has been cited as one of the reasons for crises or failures of companies over the past few years. Specific legislation, such as the Sarbanes-Oxley Act of July 30, 2002, in America, was published to rectify this problem and to restore the confidence of the public in corporate management and governance (Hurley, 2003).

Another alleged reason for corporate failures/crises is cited as the inadequate governance of the information asset (Changepoint Corporation, 2004). The board, according to the King Report (2001), has the responsibility for two main governance functions, namely directing and controlling and each of these functions depend extensively on information.
1.2 Area of Study

Information is critical to an organisation. The board, who is ultimately responsible for its success, needs to ensure that the information asset is protected adequately. This protection can be achieved through effective management and assured through effective board oversight (Institute of Internal Auditors, 2000b).

Poor corporate governance of the information asset can have disastrous effects for the organisation and its stakeholders. There have been numerous examples of corporations, over the last few years, that have suffered severe losses due to a lack of adequate governance of information technology (IT) and information security (IS), such as the scandals of Enron, Nike and WorldCom in 2001 (Alter, 2004).

Information, which is invalid or not timeous, can have serious consequences to all levels of an organisation. Information is the “lifeblood” of a company and is used by every sector and is one of its most vital assets (Institute of Internal Auditors, 2000b). The information or digital world is closely linked to the physical “brick-and-mortar” world. People populate and interact in both worlds. There are threats in the physical world, for example, a home can be robbed and there are similar threats in the digital world, for example, information can be stolen. The board and senior management are, generally, quick to protect and guard against threats in the physical world, but are they as quick to ensure the protection of their valuable information asset? (Schneier, 2000).

The data and information of an organisation need board oversight to ensure it is adequately governed. This function of information governance has been sadly lacking in the majority of companies due to lack of technological knowledge and computer literacy of board members. This is generally because information security and information technology are seen by senior management and more specifically, the board as technical issues. Consequently, this function is often delegated to the Chief Information Officer (CIO) or IT manager. This would be sufficient should the CIO or IT manager have senior management and/or board commitment and support, but often these managers are left unsupported striving, often unsuccessfully, to implement an organisational wide information security and information tech-
1.3. PROBLEM STATEMENT

The protection of the information asset needs to be an important function of the organisation, since information is critical to the success of an organisation and is one of its most valuable assets. The protection of this information asset is the direct responsibility of the board and senior management (IT Governance Institute, 2001). Information is a critical asset without which an organisation could not survive. The adequate and effective governance of this asset is equally as critical. The board and senior management have a responsibility to maintain the financial and material health of their enterprise, and this includes setting the proper direction and governance of the information asset, which includes the information technology and information security of the enterprise.

Almost all organisations are dependent on information technology to some extent and this dependence is growing daily. The board is not expected to have the technical expertise required to make decisions about the architecture of the technology of the organisation or its security and integrity. However, they are expected to oversee the necessary procedures and policies within the organisation to ensure the information asset is governed adequately. The organisation is often not staffed with proficient senior executives, who have the necessary authority, skills and resources to complete this task, which merely compounds the problem of the lack of adequate information governance.

In many cases, this has resulted in severe corporate losses or even failures, which are cited as being caused by a lack of adequate and effective corporate governance of the information asset. These corporate failures or crises could have a disastrous effect on the shareholders, staff, customers and society at large.

A number of smaller problems need to be considered to address this main problem of the lack of corporate information governance:

- What is corporate governance, its roles and responsibilities with regard to the information asset?
• Is there a lack of appreciation of the importance of the information asset by the board?

• Is there a lack of technical expertise at board level?

• Should a separate component of corporate governance be considered that focuses specifically on information security and information technology governance?

• Are the resources provided sufficient and equitable for both information technology and information security?

• Is there a reliable performance measurement and reporting system in place to ensure compliance and accountability?

• Is there a model that can be suggested that can facilitate the board in implementing an adequate process of information governance?

1.4 Objectives

The purpose of this dissertation is to investigate the system of information governance that is currently being used in many organisations to protect the valuable information asset and to suggest an improved process of corporate information governance.

1.4.1 The Primary Objective

The primary objective of this dissertation is to establish the reason or reasons why the governance of the information asset is alleged to have been the cause of many recent corporate losses and failures.

This investigation should lead to the development of a model and plans to facilitate the board in practically implementing an improved process of information governance.

1.4.2 Secondary Objective

The secondary objective is to define and examine corporate information governance and its components - information technology governance and infor-
information security governance and to indicate why these two components should be considered as governance issues and be elevated to board level oversight.

1.5 Methodology

An extensive literature study was conducted in response to these objectives. Corporate information governance, as a subset of corporate governance, was studied to establish to what extent the corporate information asset is being governed at present.

Thereafter, corporate information governance is divided into two separate components, namely information technology governance and information security governance to further investigate the governance of the information asset. The justification for the split of corporate information governance into these two components is due to the fact that each component focuses on different important issues with regard to the governance of the information asset. The information technology component focuses on the strategic planning and management of IT investment, the maintenance and development of hardware and software, risk management and ensuring IT is delivering value to the organisation (IT Governance Institute, 2003), while the information security component focuses on preserving the security of information, as it progresses through the information life cycle for capture, processing, use, storage and destruction (Ernst and Young, 2005).

Once the study of these two components was completed, the results were analysed and it was determined by valid argument and comparison:

- What their relative importance was to the governance of the information asset, and
- Whether both components should be elevated to board level oversight.

Once the literature study was completed and with all the gleaned facts at hand, a model was created to clearly explain:

- The preferred relationships which should exist between corporate hierarchical levels
- Two of the functions of the board, namely directing and controlling, and
• The activities of performance measurement, reporting and deviation analysis.

A supporting model was created demonstrating the important activities, which should be undertaken to improve the governance of the information asset.

Chapters Two and Three of this dissertation study information, corporate governance and corporate information governance and investigate their relationship.

Chapter Four and Five confine themselves to the investigation of the two identified study components, the governance of information technology and the governance of information security.

Chapter Six analyzes the data gleaned during the study and pursues the orderly gathering of the solution material, which, in Chapter Seven, enables the completion and descriptions of the two models.

Figure 1.1 represents the layout of chapters in this dissertation.
Figure 1.1: Outline of chapters in dissertation
Part II

Background
Chapter 2

Information and Corporate Governance

Chapter 2:
2.1 Introduction
2.2 Some Recent Company Failures and the Causes
2.3 The Relationship between Organisational Structure and Information
2.4 Role of Information Management
2.5 Role of Information Governance
2.6 Corporate “Sins”
2.7 Corporate Governance
2.8 Conclusion


**2.1 Introduction**

The availability of information for use within the organisational decision-making environment, has evolved dramatically over the past 60 years, due to the rapid progression of information technology (Burk, Jr. & Horton, Jr., 1988). With this rapid increase of information technology, the Chief Executive Officer (CEO) and board of directors have to be able to assimilate information at a faster rate and from a broader source. This information, if it is not adequately managed and protected, will have a profound effect on the decision-making abilities of all who use it. This, in turn, will undoubtedly lead to decisions being made and implemented, that could be detrimental to the organisation as a whole.

This chapter reviews some recent corporate failures/losses, reputedly caused by poor information and corporate governance. This is done within a framework of present practice, vis-à-vis organisational structures, the types of information utilised and management and governance roles. The section on organisational structures lays the groundwork illustrating how the various levels of management differ in their requirements for types of information. It demonstrates that each level within an organisation utilizes data or information differently to complete the tasks prescribed by their level of control or authority. This leads to a discussion on why information should be managed, and determines how information management becomes more of an information governance issue, as the corporate level of the organisation is reached and the aspect of compliance to the laws comes into play. The responsibility for information governance within the organisation is addressed to establish that it should lie squarely on the shoulders of the board and senior management. Lastly, this chapter examines corporate governance as it is practiced today, indicating some of the corporate “sins” found in many companies. It illustrates that inadequate governance of the information asset of an organisation could have far-reaching consequences, not only for the employees but for the shareholders that have invested in the company and for society at large. Society has attempted to balance the worst excesses of the free market system, by introducing legislation to protect the interests of the shareholders and the employees. One impact of this balancing act has been the imposition of personal liability on directors and senior executives, for the consequences
2.2 Some Recent Company Failures/Losses and the Causes

Much of the legislation regarding information, passed in the last few years, has been an attempt to deter the personal greed, selfishness and incompetence that has pervaded the corporate world over the last three decades (Garratt, 2003). The scandal of Enron highlighted the lack of corporate governance systems, especially from the aspect of conformance or prudent control by the board. In Enron, which was the seventh largest company of America, the information used in the accounting systems was faulty and their management used the excuse that they did not understand the off-balance-sheet accounting and had left it to their accountants. Other disasters in the United States include Tyco, WorldCom, Adelphia, and Arthur Andersen (the Enron Auditor), all in the space of four months in 2001. The reason for the bankruptcy of WorldCom was that the board did not have any financial experts on its audit committee. Their audit charter actually claimed that, because none of the committee members were financial experts, they could not be held accountable for the financial statements (Alter, 2004).

There were at least four information technology debacles, in 2001, amounting to losses of about 1.5 billion dollars (Girard, 2002). These include Nike and its 400 million dollar investment in I2 Technologies, where their projects failed due to bad vendor relationships, poor planning and strategic misdirection, project abandonment and incorrect software selection. The Internet group of Disney wrote off 878 million dollars to close down its Go.com Web portal, as it could no longer be competitive with the content and services of both Yahoo’s and AOL. Kmart wrote off 130 million dollars for supply chain hardware and software that failed to meet their expectations and further needed to replace two distribution centers at 65 million dollars. Gateway abandoned some information technology projects valued at 143 million dollars, because they no longer were aligned with their business strategies.

FoxMeyer Drug Co., as far back as 1996, stated that the failure of its Enterprise Resource Planning (ERP) system helped cause the bankruptcy of
its organisation. They spent seven years and close to half a billion dollars implementing a mainframe ERP system, stopped and started over with a client-server version (Alter, 2004).

The main reasons for these failures/losses have been cited as poor accounting and internal controls, with information as the most important component, greed and a lack of conscience from the executive and the directoral roles inside and outside the organisation (Garratt, 2003). The board and senior management displayed a lack of technical expertise and poor strategic planning, causing the loss of billions of dollars for shareholders. Invalid and poorly governed information, allied with sub-standard management at the higher levels of the organisational structure, are seen as the major reasons for these failures and losses to these companies.

2.3 Relationship between Organisational Structure and Information

Information permeates every sector of the organisation. Information is used by everyone within an organisation for many different purposes, for example, valid and timeous information enables the board of directors to make sound strategic and business decisions, leading the organisation towards its set goals. Further, information is used by the CEO to ascertain whether these strategies and goals are being met by the organisation and uses this information to report back to the board. One of the responsibilities of the Chief Information Officer (CIO) is to use information to check variance reports and deficiencies and to provide feedback to the CEO. Information is used by business unit heads, for example, to educate and train staff on the policies and procedures set by the board and senior management and to monitor their compliance (National Cyber Security Partnership Governance Task Force, 2004). This demonstrates that organisational structure has a bearing on the type of information or data required by each structural level within a company. Different levels of management require information commensurate with their responsibilities and degrees of authority.
### 2.3.1 Organisational Structure

There are many different types of organisational structures in businesses currently. The most familiar one is the pyramid type where first-line managers and employees form the base and the CEO and board of directors are at the top as illustrated in Figure 2.1. There are varying levels of middle management depending on the size of the organisation.

![Figure 2.1: The Traditional Managerial Hierarchy](image)

There are distinguishing characteristics with regard to the use of data and information within the different levels of the organisational structure (Frenzel, 1992).

### 2.3.2 Information

Information, according to Peter Drucker, is defined as “data endowed with relevance and purpose. Converting data into information thus requires knowledge. Knowledge, by definition, is specialised.” He defines knowledge as information that has been enriched by study or research and is augmented by judgment and experience (Frenzel, 1992). Both data and information are important aspects to an organisation and are utilized differently at the various structural levels. Business transactions, such as buying a car can produce
data, such as the characteristics of the car, namely its colour, whether two or four door, and size. Thus data can be defined as the objective measurement of the attributes of an entity. Names, quantities, and rand amounts recorded on sales forms represent data about sales transactions. However, a sales manager may not regard these characteristics as information. Only after these facts have been properly organised and manipulated, can meaningful sales information be given, specifying, for example, the amount of sales by product type, sales territory, or salesperson (O’Brien, 2000). The utilization of data and information, with respect to the different levels of the management, is examined to see where and how they differ.

2.3.3 The Utilization of Data and Information within the Organisational Structure

The concept of levels of management implies that there are differences in responsibility and the degrees of control or authority. These increase from the base of the pyramid to the senior executive and board (Frenzel, 1992). The responsibility differences can be distinguished by the characteristics of the data and information utilized by the different levels, and the manner in which they are used. Three characteristics help differentiate the levels of management and their information relationships and usages (Frenzel, 1992):

- The position within the pyramid or organisational structure dictates the sources of information;

- The degree of judgment involved in the application of the information varies from level to level;

- The time span in which the information is considered pertinent for making decisions equally varies per level.

Information used by the lower levels of the organisation generally has value over a relatively short time, measured in hours or days and requires relatively little judgment in its application. This is because this type of data or information is used in many companies in a data processing capacity, for example the processing of a sales order. The source of this information comes mainly from within the organisation and is in a data format rather than information. It is, usually, applied at an operational capacity. In contrast,
the information required by the CEO and board of directors, has value or meaning for a longer period of time, for example, one to five years or more. It requires a higher degree of expertise and judgment in its application, for example the CEO may need to provide business impact assessments to the company risk management process. This level of management requires information and knowledge, rather than raw data, because information brings greater understanding or meaning to the board, while raw data frequently does not. The application of information at these levels is more tactical and strategic, as illustrated in Figure 2.1. It is received as an ongoing flow of information, from a variety of external sources concerning markets, products, competitors, suppliers, technological capabilities, and personnel. It is often gathered from the Internet and from internal sources relating to the availability and suitability of the various factors of production. The board and senior management need to take long-term or strategic views, and their information therefore, often comes from outside the organisation, for example they will need information about their specific industry in order to set the company’s appetite for risk and identify risk exposure. The availability of information has proliferated and this has enabled the CEO and board to accumulate knowledge at a faster rate and from a far wider range due to the escalation in the use of technology and especially the Internet (Frenzel, 1992).

All pertinent information, according to the King Report (2001)\textsuperscript{1}, needed by employees to perform their responsibilities, should be identified, captured and communicated in a form and time frame that is commensurate with their level of management. This can include accurate, timely and relevant financial and operational data that needs to be supported by adequate and appropriate systems. These need to measure results against objectives ensuring that any variances will be highlighted. These would be reported back up the management levels to the relevant, responsible person. Therefore, it is evident that, as technology has increased the amount of information available, the need for its management and governance has increased correspondingly.

\textsuperscript{1}The King Report on Corporate Governance for South Africa 2001 was compiled by the Institute of Directors and the King Committee to investigate corporate governance in South Africa. It is considered to be an important document concerning the Code of Corporate Practices and Conduct and thus has been frequently referenced in this dissertation.
Information, its security and information technology are critical to the success of almost every substantial organisation today. They provide organisations with competitive advantage and support a substantial part of their operational capability and total value (IT Governance Ltd, 2004b). Both these assets need to be properly managed to take advantage of the opportunities provided by them.

2.4 Role of Information Management

Information management is the systematic control of various forms of information throughout all phases of the information processing cycle. The existence and maintenance of an efficient method of storing and retrieving information is critical to information processing and the reduction of time required to make informed decisions (Saskatchewan Education, 1998).

Information management, over the past century, has evolved from a concern for efficiency, within an organisation, to a concern for overall business performance; from overseeing an operations support function to performing a strategic management function. It has been suggested there are five stages in the development of Strategic Information Management as illustrated in Figure 2.2 (Burk, Jr. & Horton, Jr., 1988).

Stage One, consisting of Paperwork management which still exists, consists mainly of the management of records. Stage Two, called the Management of automated technology, focuses on the management of information technologies and technical attributes, with technical efficiency being its main business goal. Stage Three, Management of corporate information resources, focuses on the cost-effective management of information technologies and of both manual and automated information. There is a shift in objectives from both a support to a management function in business and from a focus on efficiency to effectiveness. Stage Four, named Business competitor analysis and intelligence, focuses on the business objective of gaining competitive advantage in business unit and corporate strategy. It is dependent on the quality of the intelligence analysis, information collection and processing performed by managers and staff, rather than on the use of information tools. Lastly, Stage Five is Strategic information management. This primarily focuses on corporate strategy and direction, and emphasizes the quality of decision-
2.5 Role of Information Governance

Information governance is about managing the information of an organisation and its access to it, from its inception through to its point of disposal, in a manner that is efficient and responsive to the needs of the organisation, but which is compliant with the law. Information governance is about the systems that are in place and the quality of information that is held and the
way it is accessed (Morgan-Cole, 2004). It is important that organisations keep their information secure by dealing with issues such as confidentiality, integrity and availability, as technology removes traditional barriers between themselves and their customers, partners and suppliers. Legislation, such as the Basel 11 Accord and the Sarbanes-Oxley Act of 2002, is impacting the way in which organisations use, store and protect their information (Morgan-Cole, 2004).

Some organisations, according to the Brookings Institute, gain 85% of market value of an organisation from their intangible assets while the balance is from tangible assets. The largest part of intangible assets is their information (Ernst and Young, 2000). Therefore, the need to manage and govern this asset needs to be seen as an important corporate governance function. This is achieved by ensuring that the systems for governing the information contains a series of checks and balances, which take into account the legislation and the adoption of a proper approach to issues such as email use, records management, access rights of individuals, protection of business and Intellectual Property. There has been an unfortunate lack of technological knowledge and computer literacy at board level and thus, the adequate and effective governance of the information asset has been lacking in the many companies. The main reason for this is because senior management and, more specifically, the board, consider information security and information technology to be a wholly technical issue. Consequently, they delegate this function to the CIO or Information Technology (IT) manager, without giving them the needed authority and/or resources to adequately complete this task. This frustrates the CIO and/or IT manager, while they, generally unsuccessfully, try to implement an organisational wide information security (IS) and information technology strategic plan (von Solms, 2001a).

Over the last few years, the key driver in the strategy and decision-making of an organisation has been the emergence of information technology. Information exchange, both internally and externally, has become an important issue for each organisation due to the proliferation of cheap, accessible communication via the Internet. Information technology and information security now form an integral part of the internal controls and reporting mechanisms, which are the focus of the Sarbanes-Oxley Act of 2002. The King Report on Corporate Governance states that: “.directors need to ensure that
the necessary skills are in place for them to discharge their responsibility for internal controls” (King Committee on Corporate Governance, 2002).

2.6 Corporate “Sins”

Jim Wolfensohn, President of the World Bank, stated that “the proper governance of companies will become as crucial to the world economy as the proper governance of countries” (World Bank, 1999). Proper governance is about the balance between performance and conformance, because conforming to corporate governance standards results in constraints on management. Boards have to balance constraints on management with performance for financial success and the sustainability of the organisation’s business. Tomorrow’s Company in the United Kingdom defined the concept of three corporate “sins”, namely sloth, greed and fear. Sloth was defined as being the loss of flair or risk-taking when an organisation gives way to administrative burdens, and the executives become “lazy” and no longer take the risks necessary to achieve competitive advantage. Greed is defined as when executives might take a short-term decision, because it has greater impact on their share options and bonuses, over a decision that might create longer term prosperity for the company. Lastly, fear is defined as when the executives become subservient to shareholders and ignore the drive for sustainability and enterprise (King Report, 2001).

Corporate governance principles were developed, amongst other reasons, because shareholders and investors were concerned about the excessive concentration of power in the hands of management. This protection against greed could encourage the “sins” of sloth and fear, with the erosion of organisational enterprise and the encouragement of subservience. There is definitely a need for balance and this is achieved through effective corporate governance (King Report, 2001).

2.7 Corporate Governance

What is corporate governance and what is its importance for the organisation? These questions will be examined to obtain a better perspective of where information governance fits into the overall corporate governance
strategy.

2.7.1 Corporate Governance History

Corporate governance systems have evolved over time, generally in response to corporate failures or system crises. Each crisis or major corporate failure, often a result of incompetence, fraud, and abuse, was met by new elements of an improved system of corporate governance. Developed countries have established a complex system of laws, regulations, institutions, and implementation capacity in government and the private sector through this process of continuous change. Their objective was not to hold organisations back but rather to balance the promotion of enterprise with greater accountability. The enforcement of these laws and regulations created a culture of compliance and encouraged organisations to improve their management style to attract human and financial resources on the best possible terms. There came an increasing diversity and complexity of shareholders and stakeholders through this process of continuous change. Globalization forced many organisations to look for international finance and thus, faced greater competition (World Bank, 1999).

A healthy and competitive corporate sector is increasingly fundamental for sustained and shared growth; sustained because it will be able to withstand economic shocks and shared because it delivers benefits to all society. Corporate governance is equally as important to the private sector as overall governance is important to the public sector. Good governance of organisations should be seen as a source of competitive advantage and is critical to economic and social progress. Corporate governance has only recently emerged as a discipline in its own right (World Bank, 1999).

2.7.2 What is Corporate Governance and what is its importance?

Often the interests of those who have effective control over an organisation can differ from the interests of those who supply the company with external finance. An organisation that lacks the protections that good governance supplies, implies for its investors, who lack control over the organisation, that it is risky and costly to protect themselves from the opportunistic behaviour
and greed of senior executives and/or controlling shareholders.

Corporate governance can be defined from two perspectives. The first is the corporate perspective, which indicates that corporate governance is about maximizing value, subject to meeting the financial and other legal and contractual obligations of the corporation. This stresses the need for the board of directors to balance the interests of shareholders with those of other stakeholders, which could include employees, customers, suppliers, investors and communities, to achieve long-term sustainability. The second is from a public policy perspective. From this viewpoint, corporate governance is about nurturing an enterprise, while at the same time, ensuring accountability in the exercise of power and patronage by companies. The role of public policy is to provide organisations with the incentives and discipline to minimize the divergence between private and social returns and to protect the interests of stakeholders. There is a balance between the internal incentives, which define the relationship among the key players in an organisation, and the external forces, namely policy, legal, regulatory and market forces, that together govern the behaviour and performance of the organisation (World Bank, 1999).

Corporate governance is, therefore, about balance - balance between economic and social goals, between individuals and communal goals and encouraging the efficient use of the organisational resources and being held accountable for their stewardship. Its main aim should be to align, as nearly as possible, the interests of individuals, corporations and society (World Bank, 1999).

2.7.3 Functions of Corporate Governance

One of the primary functions of the board is achieving this balance, which it does by directing and controlling the organisation. Directing is an intellectual activity showing the way ahead and giving leadership, while keeping the organisation under prudent control, by means of internal controls and a set of policies. The board needs to determine the policies of the organisation in relation to its changing external, macro-political environment. Strategies need to be derived from these policies, which lead to the broad deployment of the scarce organisational resources to deliver its objectives. At the same time, the board has a legal fiduciary duty to hold the company in trust on behalf of
the owners by ensuring that there is sufficient oversight of the management
performance systems. They need to know the current and future positions of
the organisation, so that deviations can be assessed and resources allocated to
correct any deviations (Garratt, 2003). P Weill (2002) put it very succinctly,
“Don’t Just Lead, Govern!...Governance leverages the ingenuity of all the
enterprise’s people, not just the leaders, while ensuring compliance with the
overall vision and principles.” (Weill & Broadbent, 2003).

The King Report (2001) recommends that four central pillars, namely,
accountability, responsibility, fairness and transparency, are required by an
organisation to provide effective corporate governance. *Accountability* en-
sures that those individuals or groups within an organisation, who make
decisions and take actions on specific issues, are accountable for both. Mech-
anisms must exist and be effective to allow for accountability. Reporting and
disclosure are two functions that are fundamental to corporate governance for
accountability and both depend extensively on information. *Responsibility*,
in the management context, relates to the behaviour that allows corrective
action and penalises mismanagement and misconduct. *Transparency* enables
the shareholders and other stakeholders to be well informed and enables
them to make significant assessments about the actions of the company, its
economic fundamentals and any non-financial aspects relevant to it. They
must receive comprehensive financial reports and have access to other perti-
nent information to achieve this. These reports must have integrity and the
disclosure must be timely and balanced (Corporate Governance Task Force,
2003). Good internal controls need to be implemented to ensure their in-
tegrity. *Fairness* allows for balance within an organisation. The rights of
various groups have to be recognized and valued (King Report, 2001).

The lack of internal controls over financial reporting has been stated as
one of the main reasons for the failure or loss of many organisations in the
past. The Sarbanes-Oxley Act of July 30, 2002 in the United States of Amer-
ica was published to rectify this problem and to restore the confidence of the
public in corporate management. US Attorney Gary Saidman stated “It’s
hard to sign off on the validity of data if the systems maintaining it aren’t
secure, then internal controls are not going to be too good.” (Hurley, 2003).
It is, therefore, imperative that the infrastructure of the systems be examined
to ensure that they are secure. It is equally important to realize that cor-
2.7. CORPORATE GOVERNANCE

Corporate governance is not merely about compliance with legislation but it is essential for the board to establish a climate of trust and confidence through oversight (World Bank, 1999). How does the board create this climate of trust and confidence within its organisation?

2.7.4 The Roles and Responsibilities of the Board

The Organisation for Economic Co-operation and Development (OECD) (2004) maintains that corporate governance should ensure the strategic guidance of the company, the effective monitoring of management by the board and its accountability to the company and the shareholders. It should promote transparent and efficient markets, be consistent with the rule of law, and clearly articulate the division of responsibilities among different supervisory, regulatory and enforcement authorities.

There is emerging a greater need for corporate transparency and accountability where companies, for the first time, make themselves clearly visible to shareholders, customers, employees, partners and society. More transparency engenders a climate of confidence and trust, and likewise, a lack of transparency can result in a lack of trust in a company. The building of transparency into corporate governance increases confidence in the processes and procedures of a company, because these processes and procedures are clearly visible and nothing is being hidden. Connectivity makes information available when and where it is needed by a company and this is the nature of doing business today. Companies are linked through the Internet and other public networks providing this availability to suppliers, customers and business partners and they are connected to virtually everyone in the world. This need for connectivity, availability and transparency exposes information to risks outside the control of the company and sound infrastructures and information security policies need to be in place to protect the health and future of the organisation’s information asset of the organisation (Institute of Internal Auditors, 2000b).

The health and future of the information asset and the entire organisation depends on good direction from the board and it is essential for the board to be aware that each member is corporately and personally responsible and liable financially for the duties and tasks of the board (Garratt, 2003). Bob Garratt in his book ‘The fish rots from the head’ discusses the roles of a
board by pointing out that there are four directoral dilemmas.

These directoral dilemmas give an insight into the balancing act required by a board (Garratt, 2003):

- The board must simultaneously be entrepreneurial and drive the business forward whilst keeping it under prudent control. Thus, the board has to be adventurous and risk-taking to keep up with the changes in the external environment and yet, has a responsibility to hold the company in trust on behalf of the owners;

- The board is required to be sufficiently knowledgeable about the workings of the company, to be answerable for its actions and yet, needs to stand back from the daily management and retain an objective, longer-term view. They need to develop a *helicopter view* ability necessary for its direction-giving function;

- The board must be sensitive to the pressures of short-term, local issues and be informed of the broader trends and competition, even of an international nature;

- The board is expected to be focused on the commercial needs of the organisation, whilst acting responsibly towards its employees, business partners and society as a whole.

Each role mentioned above, ironically, seems to be a contradiction of itself but still needs to be balanced by the board to provide adequate governance for the organisation. All of the above roles of the board use information in some form or another. This information needs to be valid, timeous and accurate to enable the board to fulfill its roles and responsibilities.

Figure 2.3, adapted from Bob Garratt’s book by indicating the directing and controlling functions, illustrates corporate governance and its roles and responsibilities. It demonstrates that the corporate governance policy/foresight function should lead to strategic thinking, which is part of the directing component of corporate governance. The controlling component includes management supervision and accountability (Garratt, 2003).

Managers can potentially add significant shareholder value simply by developing good governance practices. A survey by McKinsey and Co. in
2.7. CORPORATE GOVERNANCE

Figure 2.3: Corporate Governance, its Roles and Responsibilities

2000, indicate that there is a willingness to pay a premium for the shares of a well-governed company over one considered poorly governed, even with comparable financial records (King Report, 2001).

The OECD Principles (1999) states that “corporate governance should ensure that timely and accurate disclosure is made on all material matters regarding the corporation, including the financial situation, performance, ownership, and governance of the company.” This promotes good governance principles. Good governance, in turn, depends on information flow, therefore where does the responsibility for this information asset lie?

2.7.5 The Responsibility for Information Governance

Some quotes on corporate governance taken from reputable institutions, will help determine where the responsibility for the information asset of the organisation should reside.

The King Report (2001) maintains that “information technology now forms an integral part of internal controls and reporting information. At the same time, there are fiduciary implications because of the electronic formation of contracts, the integrity of electronic communications, the retention of records etc. Consequently, directors need to ensure that the necessary skills
are in place for them to discharge their responsibility for internal controls.”

The reliability of financial reporting is dependent on a well-controlled information technology environment.

Organisation for Economic Co-operation and Development (2004) state that “The corporate governance framework should ensure the strategic guidance of the company, the effective monitoring of management by the board, and the board’s accountability to the company and the shareholders. To achieve this, the board should ‘ensure the integrity of the corporation’s accounting and financial reporting systems, including independent audit, and that the appropriate systems of (internal) control are in place’...”.

The Institute of Internal Auditors (2000) states that “the information possessed by an organisation is amongst its most valuable asset and is critical to its success. The board of directors, which is ultimately accountable for the organisation’s success, is therefore responsible for the protection of its information. The protection of this information can be achieved only through effective management and assured only through effective board oversight.”

The statements above directly link corporate governance with the protection and governance of the information asset. They all indicate that good corporate governance includes total commitment and responsibility towards the information asset (von Solms, 2001a). Therefore, the responsibility for information governance lies squarely on the shoulders of the board of directors.

2.8 Conclusion

All these disasters discussed at the beginning of this chapter, indicate weak corporate governance and board-level guidance, both financially and due to problems of information technology infrastructure, poor planning and strategic mis-direction. These failures or crises indicate that, even though the responsibility for information governance resides with the board of directors, the function is not being performed adequately. It is important to realize that should the consideration of the board for information technology and security be deficient, then the whole organisation, including the board, the senior management team, employees and shareholders, will be totally dependent on the CIO to ensure that the governance of the information asset
exists at the departmental level (Changepoint Corporation, 2004). The placing of information governance at this level will not benefit the organisation, because they do not have the authority and control that is required. This results in the function of direction and control of the board, with regard to information, being non-existent and leaves the information asset in a poor predicament.

The board of directors are expected to adequately govern and protect this important asset but how can they take responsibility for an entity they do not understand and how can they be held accountable for technology that is so specialised? An answer to this dilemma could lie with the implementation of a specialised subcomponent of corporate governance within the organisation, to oversee this important function. A deeper look into this subcomponent of corporate governance, called corporate information governance, will show the feasibility of this proposal.
Chapter 3

Corporate Information Governance
3.1 Introduction

Poor corporate governance can have disastrous effects for the organisation, the shareholders and the organisational publics. The corporate failures/losses referred to in the previous chapter, indicate that there is something seriously lacking in the present structure of corporate governance.

This chapter examines the reasons for this serious lack of sound information governance within the present structure of corporate governance. A definition of corporate information governance will be proposed using the literature available. The objective of this is to gain a deeper understanding of what corporate information governance actually means. It is proposed that corporate information governance be divided into two components, namely information technology governance and information security governance, for the purpose of this dissertation.

In pursuance of this objective, the importance of both of these components as separate governance issues will be illustrated and the commonality that exists between them.

A proposal is presented to close the circle for the elevation of corporate information governance from its present position, to one from which many of the current ills can be more effectively dealt with, to the benefit of the organisation as a whole. This is achieved by addressing the structuring of the corporate information governance responsibilities and indicating why corporate information governance should not be addressed by existing board committees but instead by the CIO with a seat on the board.

3.2 Corporate Information Governance Defined

As an enterprise increases its dependence on IT and on accurate, secure information for success, it equally increases its dependence on the people that manage and govern this asset (Frenzel, 1992). It would seem that specialised responsibilities with regard to the information asset for the board and senior management may contribute meaningfully to a reduction of corporate failures or crises due to information mismanagement. Corporate information governance, its components and structure need to be defined to evaluate this
3.3. COMPONENTS OF CORPORATE INFORMATION GOVERNANCE

concept.

The new component of corporate governance being proposed, called corporate information governance, will be defined as the governance and protection of all information, in its electronic and paper-based forms, flowing into, within and out of an organisation. This corporate information governance is achieved by implementing checks and balances throughout the entire organisation to ensure the authenticity and security of the information; the management of risk; and the disciplined management and planning of information technology investment decisions and IT projects; the responsible use of IT resources; and performance monitoring.

Corporate information governance needs to co-ordinate all the activities relating to information governance throughout the entire organisation, ensuring that the strategies and goals of the board are cascaded down throughout the organisation and that compliance is measured and reported back. It needs to include the assigning of decision-making rights, a corporate responsibility matrix and modular activity plans, which will be discussed in detail in Chapter Seven, to encourage adequate governance and desirable behaviour in the use of the information asset within a company.

3.3 Components of Corporate Information Governance

It can be assumed from the literature study and definitions on the previous page, that the corporate information governance can be divided into two major components, for the purpose of this dissertation. The first component is the information technology (IT) component, which focuses mainly on strategic planning and management of IT investment, the maintenance and development of hardware and software, risk management and ensuring IT is delivering value to the organisation (IT Governance Institute, 2003). The second component is the information security (IS) component, which focuses on preserving the security of information, as it progresses through the information life cycle for capture, processing, use, storage and destruction (Ernst and Young, 2005). It needs to focus on strategic planning with regard to IS, ensuring that IS delivers value to the organisation, that the risks are
managed and overseen by the board, and that the resources are managed adequately. Each of these components needs to be examined to establish their incorporation as governance issues.

### 3.3.1 Why should information technology be considered a governance issue?

Every business, non-profit organisations, and the economy of any developed country, depends on the continuous operation of information technology. Electrical power grids, railways, airlines, banking and financial systems, oil and gas and telecommunication networks are prime examples and each of these are dependent on information technology in one way or another. The exponential growth of connectivity has created new information and risk vulnerabilities that can cause the failure of businesses that would have otherwise been sound (Institute of Internal Auditors, 2000a).

Information technology is utilised by every sector of an organisation and vast amounts of money are being invested in new and updated technologies to increase its speed and productivity and, ultimately, the shareholder value. The money being invested necessitates board-level risk management and governance activities for IT. According to Changepoint (2004), CEOs and CFOs can face prison terms for violating corporate governance mandates and this indicates an increased need for the oversight of IT investments at board level. Most companies spend more than 50% of capital expenditure on IT investments but roughly 6% of publicly traded companies in the United States of America have IT representation at board level. Executive management teams are often disillusioned by the lack of returns from IT investments and there is increasing focus on the measurement and maximisation of the value to be gained from these investments. IT governance needs to be established and delivered within an organisation because this helps ensure that their technology investment is aligned with the top-level business objectives (Changepoint Corporation, 2004).

Ron Exler, an analyst with Robert Francis Group, maintains that corporate governance and IT governance “are now intimately intertwined. The increased scrutiny on corporate governance directly and indirectly affects IT and the direction IT governance will take.... Furthermore, in an era where
technology is critical to business, corporate governance is incomplete without adequate IT governance” (Changepoint Corporation, 2004).

Information technology can provide great opportunities for an organisation to attain strategic advantage and economic success but simultaneously can present the organisation with major risks. The management of risk, specifically related to IT, has become increasingly important due to the vast amount of investment in IT, the increase in risk due to new technologies and the extensive use of networks and the Internet (Changepoint Corporation, 2004). The King Report (2001) states that for senior management to discharge their governance responsibilities, they need to address the increased risks and challenges introduced by the technology used by the organisation.

The primary drive for corporate governance has been the need for transparency of enterprise risks and the protection of shareholder value. The use of technology throughout the organisation has created a critical dependency on IT that calls for a specific focus on IT governance. The aim of IT governance is to ensure that expectations for IT are met and that the IT risks are appropriately mitigated (IT Governance Institute, 2003). According to the King Report (2001), the board is responsible for ensuring that their technology resources are adequate to accomplish the business activities of the organisation.

All these factors point towards incorporating IT governance at board level under a leader, who has the authority and ability to ensure all facets of the information technology of the enterprise, including its risks, are governed adequately and appropriately to maximise the return on investment for the organisation.

3.3.2 Why should information security be considered a governance issue?

Information technology plays an integral role in the receiving, storage, processing and transmission of the information asset of the organisation. Information, per se, plays a vital role within the business structure and therefore, its protection and security should be considered a top priority by the organisation. Information security cannot merely be viewed as a technical issue (Changepoint Corporation, 2004), but needs the attention and com-
mitment from both senior management and the board. Swindle and Connor (2004) states that information security needs to be “embraced as a corporate governance responsibility that involves risk management, reporting controls, testing and training, and executive accountability. As such, it requires the active engagement of all CEOs and boards of directors”.

Some of the reasons given by Ernst and Young (2005) for the board to be concerned with information security are:

- Enabling business strategy: Information security increasingly becomes vital to an organisation in creating and sustaining trust between organisations and their business partners, customers and employees and it means that a strong alignment between business, technology and information security strategies is required;

- Sustaining normal business operations: The value of the information within an organisation increases as do does the threat of theft, fraud and attack. Important business information may be lost or corrupted due to inadvertent and accidental events that damage the information systems and result in the key business processes to become unavailable;

- Managing risk: Risk management improves and contributes to improved governance and executive decision-making ability and allows the company to leverage risk and be more competitive in exploring new business opportunities. The management of information security risk is a key aspect in achieving this;

- Avoiding unnecessary costs: The lack of information security generally results in business and IT process inefficiencies, lost productivity and poor customer service. A loss of reputation due to publicised information security incidents will, more often than not, lead to the need for significant marketing and brand protection expenditure;

- Legal liability: Security breaches create a variety of litigation risks and this can lead to the organisation facing legal liability;

- Meeting compliance requirements: The need for sound risk processes within business as suggested by the King Report, means that it is essential that the organisation focus on developing, implementing and
sustaining sound information security risk processes. The board has a fiduciary responsibility for implementing sustainable risk management processes and meeting corporate governance requirements;

- Investing for success: Information security is a strategic, business issue and the organisation may fail to realise any meaningful business value should the board and senior management not direct the development and deployment of the information security strategy.

Information security governance relates to the security of information systems and how this is dealt with at an executive level. The increased need for growth and sustained competitive advantage means companies need to provide access to their information and services. There is a constant balancing act being performed within organisations to be open, transparent and accessible while complying with the myriad of governmental regulations concerning information, for example, the Electronic Communications and Transactions Act (ECT Act), the Sarbanes Oxley Act and the Health Information Portability and Accountability Act (HIPAA). This balancing act depends on secure information systems. Openness and accessibility produce their own inherent risks, for example, risk of theft, alteration, interception and dissemination of confidential data, as well as fraud, loss of reputation and economic loss. Companies must elevate information security to a corporate governance level to systematically strengthen it (Entrust, 2004b).

The board is responsible and accountable to the shareholders and they must ensure that their company produces value and delivers a suitable return on investment (King Report, 2001). The assurance of the security of business information enables the company to generate a suitable return because they will be creating a safer business community internally and for their customers and others connected via their network (Swindle & Connor, 2004). According to Swindle and Connor (2004), good information security governance will provide more than just legal or compliance benefits, but could serve as a “catalyst to even greater productivity gains and cost efficiencies for businesses, customers, citizens and governments during times of crisis and normal operations.”

The Corporate Governance Task Force (2004) states that “the road to information security is through corporate governance”. Information security
is often viewed as a technical issue but it is also a governance challenge that involves risk management, reporting and accounting.

### 3.3.3 How do the components of information technology and information security governance combine within corporate information governance?

It is evident from the previous sections that risk is a common problem in both of these components. Risk management is an important aspect of both IT and IS and is officially a board responsibility. The question of how much security is enough, given the level of access required, and what protection is most beneficial to the company from a cost perspective, needs constant attention. It is not possible to have a 100% risk free organisation. Risk needs to be managed according to the appetite for risk of the enterprise. Risk appetite defines the quantity and nature of risk that an organisation is willing to accept, as they evaluate the trade-offs between perfect security and unlimited accessibility (Whitman & Mattord, 2003). This appetite for risk is decided at board level. Risk management is practiced throughout the organisation by everyone in their daily activities but it is ultimately the responsibility of the board (King Report, 2001). Risk management is both a driver and an element of governance. Proper governance reduces risk exposure that potentially could cost the organisation, provides an information base for informed decisions, and furnishes a comprehensive and yet flexible framework for planning (Exler, 2003).

There are risk factors linked to both components, which will be addressed in the next two chapters. These, however, differ but they need to be addressed and managed and ultimately this management is the responsibility of the board. The two components of corporate information governance address different issues, one concerns the technology and the other the security of the information itself. They are issues of equal importance to the survival of the organisation. These two components are set alongside and overlap specifically in the risk management area, which as stated previously is a common problem for both components, and needs to be addressed by the board in order to ensure the sustainability of the organisation.

Figure 3.1 illustrates how these components of corporate information gov-
3.4. Structuring Corporate Information Governance Responsibilities

Organisations are staffed by people. People, at all levels, can be obstructive and show negativity towards the creation of anything new. This is especially true when the creation is perceived to be invasive of their area of expertise.
or control. All divisions within a corporation use the information asset, and some division heads may see the creation of a corporate information governance structure, with overall responsibility for the information asset, as an invasion of what previously was considered to be their information (Frenzel, 1992).

It is commonly believed by upper management and directors that the members of an organisation will expend great effort to avoid acceptance of responsibility when guilt for corporate failure is being assigned. For example, the board of WorldCom stated that they did not have any financial experts on their audit committee and their audit charter claimed that because none of the committee members were financial experts, they could not be held accountable for their financial statements (Alter, 2004).

Who then should be responsible for this corporate information governance? Should it be the responsibility of a committee? The King Report (2002) recommends the following board committees to facilitate the board with corporate governance:

- Executive Committee;
- Audit Committee;
- Remuneration Committee;
- Nomination Committee;
- Employment Equity and Skills Retention Committee;
- Environment, Health and Safety Committee;
- Risk Management Committee.

The two committees, which can have a bearing on information governance are the Audit or Risk Management Committees. A brief overview of their functions and roles as specified by the King Report will indicate which, if either should be held responsible for corporate information governance.

An Audit Committee, in most organisations, is responsible for reviewing the financial aspect of information technology investments, with slight regard for the broader issue of information security and information technology governance. Many of these Audit Committees are staffed by finance/accounting
personnel who normally have scarce or no in-depth knowledge of IT or the means needed to adequately secure the information flowing through the organisation. Both of these aspects are essential for a sufficient understanding of strategic IT and IS issues, which are important elements of corporate information governance (Changepoint Corp, 2004). New regulations such as the Sarbanes-Oxley Act of 2002, have caused these committees to assume new and demanding duties and responsibilities, leaving them less time to focus on information governance and this further dilutes these Audit Committees in effectively managing their information asset.

Janice Wilkins, Director of Internal Audit at Intel, states, as confirmation of the above, that even though most audit departments are comprised of operational auditors and technical IT auditors, she does not believe that the operational auditors can effectively evaluate the processes of the organisation without a basic understanding of IT. This is because they lack the sufficient competencies to evaluate general controls such as data, physical and access security, database administration, applications, network and IT infrastructure controls (Institute of Internal Auditors, 2001). This is borne out by the King Report (2002), where the responsibilities and functions of the Audit Committee are mainly financial with no reference to IT. Should the Audit Committee, therefore, be responsible for overseeing IT direction and control? This function is vitally important to information governance.

The Risk Management Committee, on the other hand, focuses entirely on risk management issues: such as technology, human resources, credit and market, disaster recovery, operational and lastly, compliance and control risk. The King Report (2002) does not suggest that an IT person should serve on this committee, which is an essential requirement for adequate and effective information governance, as illustrated in previous sections. There is no direct reference to information technology governance in their responsibilities and functions. Would the risk management committee be in a position to sign-off the IT internal control systems and procedures? This function is not part of the responsibility of a Risk Management Committee but is a responsibility of information governance.

There is a need for the governance of information at a much broader level to oversee the following aspects: IT strategic planning, risk management, IT expenditure and value delivery, IT resource management, performance
measurement, potential disasters and information security.

There is an old adage that there can be no accountability without responsibility and no responsibility without authority. It is proposed that the CIO, charged with specific responsibility for the overall information asset, should have a seat on the board to prevent corporate ‘buck passing’ as previously described, from contributing to corporate failures or losses and to ensure that proper accountability with commensurate responsibility and authority is implemented. This seat on the board would grant sufficient authority to the incumbent ensuring the successful execution of his/her duties and responsibilities. The CIO will be held responsible for the information technology and information security governance of the company, even though most of the IT resources are consumed outside the information division, as the chief financial officer of the enterprise is held responsible for the organisational expenditure (Frenzel, 1992).

The very nature of the task overseen by the CIO is such, that the incumbent should be a person of broad experience with good leadership skills and business acumen because he is responsible for the implementation of an organisational wide information security and information technology strategic plan (von Solms, 2001a). He/she is required to have excellent communication skills encouraging dialogue between operational divisions (Changepoint Corporation, 2004). Lastly, he/she needs the ability to inform and advise top management on the emerging IT opportunities, be able to incorporate these opportunities into the business strategies and plans and be able to market IT accomplishments to the board (Frenzel, 1992).

Figure 3.2 illustrates the proposed structuring of a corporate information governance responsibilities within an organisation.

Corporate information governance, as demonstrated in Figure 3.2, has been elevated from its present position, to a board position with full responsibility for the information asset, even though the CIO still has line responsibility to the CEO. A reciprocal staff relationship must exist between the operational divisions to ensure the unhindered access to all information. This enhances the opportunities of the proposed new CIO opportunities to succeed in his/her tasks. This dual relationship is often found in corporations with operational divisions having a staff function on the board, for example, advising on strategic matters, and a line responsibility to the CEO,
for example, reporting on actual versus budget achievements (Frenzel, 1992).

The CIO should, on occasions, as changes occur within and without the organisation, elicit the help and advise of external, specialised IT consultants, providing independence of thought (King Committee on Corporate Governance, 2002). Organisational changes often fuel much of the innovation in product development, marketing, sales, and service currently. The ability of the CIO to support technological adaptation, often in consultation with outside IT specialists, to find new and more effective ways to do business, is driven by competitive pressures and the need for improved productivity (Frenzel, 1992).

The CIO needs to be a technological leader of the company and provide for its business needs in the selection and introduction of new technologies that will create opportunities and competitive advantage. Amongst other things, he/she must ensure that the IT strategic plans are constantly aligned with the business strategies; must ensure that the security of the information is kept intact; and that the information required by the different organisational divisions and the board is timeous, valid and accurate.
3.5 Conclusion

The ability of corporations to improve the governance of the information asset has not kept pace with the ever-increasing demand for information, its security and access, which has resulted from the rapid technological advances made in the information arena.

Many corporate failures or crises are the result of poor information governance, as discussed previously. It is established that corporate information governance is more important than generally accepted and to gain a better understanding, it should be divided into two components, information technology governance and information security governance. A proposal has been put forward, which will enable corporations to improve the governance of their information, by ensuring that the CIO, with board representation, is charged specifically with the responsibility for the proper governance of this asset, both from a technological and a security perspective.

The understanding of corporate information governance function will be facilitated by an in-depth examination, in the next chapter, of its two components, namely the governance of information technology and the governance of information security.
Chapter 4

The Governance of Information Technology

Chapter 4:
4.1 Introduction
4.2 Aspects of Information Technology
4.3 Why is Information Technology Important?
4.4 The Elements of Information Technology Governance
4.5 Objectives and Purposes of IT Governance
4.6 Proposed IT Governance Process
4.7 Conclusion

Chapter 1
Introduction

Chapter 2
Information and Corporate Governance

Chapter 3
Corporate Information Governance

Chapter 4
Governance of Information Technology

Chapter 5
Governance of Information Security

Chapter 6
Core Aspects and Fundamental issues

Chapter 7
A Corporate Responsibility Matrix

Chapter 8
Conclusion
4.1 Introduction

Corporate failures or losses, due to poor governance of the information asset, bring serious consequences. This statement poses the following questions:

- “Why is the information asset poorly governed?”
- “What can be done to improve the governance of the information asset?”

It has been assumed in an endeavour to answer these questions that there are mainly two components of corporate information governance, namely the governance of information technology and the governance of information security. The importance of each warrants individual study to further our understanding of the roles they play and to ascertain the place of each in the overall subject of corporate information governance.

This chapter confines itself to a more in-depth study of the governance of information technology, from the evolution of technology itself to a definition of information technology governance and some related aspects. A discussion of the reasons for the importance of information technology governance will be followed by an overview of its various elements. Lastly, a proposal follows which outlines a process whereby the function of information technology governance can be improved.

4.2 Aspects of Information Technology

The governance of the information asset has needed to evolve to adapt to the change in the requirements for information within an organisation, so too has information technology and its governance. The growth in information technology has been a blessing for many people. The technology has formed a major part of their formal education and a basis for their employment. It has been a platform on which their future depends. Alternately, for others, information technology has been a complicating factor, which is to be feared or at least viewed with apprehension. It has brought change for nearly everyone.
4.2. The Definition of Information Technology

The definition of information technology from the Oxford Dictionary is “the study or use of systems such as computers and telecommunications for storing, retrieving and sending information” (AskOxford, 2005). It includes the use and management of all the hardware used in an organisation to store, retrieve, process and send information and data, such as computers, servers, networks, as well as the IT support systems, for example applications, operating systems, protocols, and utilities that are involved in this process.

Technology in the current global market, is one of the most important vehicles which enables business operations. Information technology is used from boardroom level to the mail room, for example, deals are made, goods shipped, client accounts tracked and inventories kept of company assets, all by means of IT. Dr Whitman et al. (2004) defines IT as “the vehicle that stores and transports information - a company’s most valuable resource - from one business unit to another.” The failure of this vehicle can result in business deals being lost, shipments not sent, and the assets of the organisation becoming vulnerable to external and internal threats.

4.2.2 The Evolution of Information Technology

It is often thought that the evolution of information technology began with computers. This is not true. In reality, the first use of technology to process information was probably the invention of the earliest mechanical typewriters.

Man quickly realised that he could do ‘more’ and ‘more quickly’ by applying machinery/technology to information and the accounting machine era began. The next step in the evolutionary process was the application of pure electronics to process information. This saw the invention of ‘bits and bytes’ technology, the fundamentals of which are still in use today. The major route of the information technology evolution, subsequently, has been the use of chip technology, whereby increasing amounts of information are ‘processed’ by ever decreasing sizes of equipment.

Information technology has evolved from simple stand-alone batch application computer systems used by single-users into ones capable of multi-tasking and distributed processing in a distributed environment. The envi-
4.2.3 The Purpose of Information Technology

The purpose of information technology according to the IT Governance Institute (2003), is essentially to manage the transactions, information and knowledge necessary to initiate and sustain economic and social activities.
4.2. ASPECTS OF INFORMATION TECHNOLOGY

IT has become an integral part of the business in most organisations and is fundamental to support, sustain and grow the business.

Other purposes of IT, besides the managing of information, are to improve productivity and reduce costs which can, in turn, contribute to competitive advantage. IT is fundamental for managing enterprise resources, dealing with customers and suppliers and enabling transactions that are, increasingly, more global. IT is critical for recording and disseminating business knowledge. Information technology is not a static technology and the speed of innovation and of deployment of IT within an organisation can either create or destroy competitive advantage. Information technology is fundamental to the strategic success of an organisation, whether an organisation is using Enterprise Resource Planning (ERP) or Customer Relationship Management (CRM), Sales Force Automation (SFA) or e-Commerce.

4.2.4 The Expectations for Information Technology

The expectations for IT, from an organisational point of view, include an increase in automation thereby making the organisation more effective. IT is expected to decrease the overall cost of the business operation and increase the profitability of the company. The expectations of the board, according to the IT Governance Institute (2003), with regard to information technology, include delivering ”value to the business by providing fast, secure, high-quality solutions and services, generating reasonable returns on investment, and moving from efficiency and productivity gains toward value creation and business effectiveness.”

Another expectation from IT is that it can be used to manage risks by implementing adequate security, reliability and compliance measures to the information asset. Much attention has been focused on IT with the increase in regulation concerning financial reporting, such as the Sarbanes-Oxley Act (SOX) of 2002, because it is the foundation of an effective system of internal control over financial reporting (IT Governance Institute, 2004).

Lastly, information technology is expected to assist with the facilitation of compliance to legislation. The board cannot merely ask questions of management to comply with legislation. They must take further measures and ensure that there are monitoring and measurement procedures in place. These must be effective and appropriate to perform an effective oversight function. In-
formation technology can be used effectively in this regard. Generally, very few board members have the expertise to evaluate whether the procedures in place, are effective and appropriate. The complexity of IT and the intangible value of information makes IT a more difficult area to govern.

4.3 Why is Information Technology Important?

Information technology is important in many areas of an organisation, for example, managing its resources, dealing with suppliers and customers and enabling large amounts of information to be transacted both locally and globally. It is equally critical for recording and disseminating business knowledge. A large amount of the market value of an organisation has changed from being tangible, for example, inventory and facilities etc. to being intangible, for example, its information, knowledge, expertise, reputation, trust and patents etc. Much of the intangible assets revolve around the use of IT. Therefore, the management and governance of this important asset is vitally important.

There are a number of reasons for the importance of IT, some of which include (IT Governance Institute, 2003):

- IT is critical to the organisation;
- IT is strategic to the organisation;
- Expectations for IT and reality do not match;
- IT has not received the attention it deserves;
- IT involves huge investments and large risks.

These reasons are discussed to see how they impact on the management and governance of information technology.

4.3.1 IT is critical to the organisation

This criticality arises from the increasing dependence on information, and the systems and communications that deliver it. Today, the utilization of IT has the potential to be the major driver of economic wealth. Richard Nolan,
a Harvard Business School Professor, states that the most important reason for the board and senior management to be involved in IT, is because the role of IT is expanding both “deep within organisations and across organisations” and that decisions affect entire networks of companies, as “every organisation today is absolutely dependent upon IT.” (Alter, 2004).

The dependence of most organisations on technology has grown so rapidly that technology disruption has become one of the requisite components when calculating operational risk. This was highlighted during the September 11, 2001 attack on the World Trade Centre by terrorists, who hoped to cripple the American economy. Lloyd’s of London estimated that there was an estimated 10 billion dollar in corporate losses, directly related to the business interruption that the World Trade Centre attacks caused (Sungard Availability Services, 2004).

### 4.3.2 IT is strategic to the organisation

Senior management and the boards of organisations are repeatedly realising the strategic value of IT and its significance on the success or failure of their organisation and therefore, are striving to successfully leverage IT opportunities for its competitive advantage. It is important for the board to know whether their IT is likely to achieve its objectives and be resilient enough to learn and adapt to changes and growth. They need to know that the risks are being managed judiciously and lastly, whether appropriate opportunities are being recognised and capitalised on (Trites, 2004).

### 4.3.3 Expectations for IT and reality do not match

The managing and investing in IT means that some expectations of the board and senior management for IT include its harnessing and exploitation to deliver business value. IT is expected to provide fast development with appropriate quality and the necessary embedded security. It is assumed that it is easy to ascertain that IT investments have a quantitative return and that IT will provide ‘more with less’. Lastly, the expectations for IT are that it will move the organisation from efficiency and productivity gains towards value creation and business effectiveness (IT Governance Institute, 2003).

The reality can be vastly different. Organisations often experience busi-
ness losses, reputational damage or a weakened competitive position due to poor management decisions. Its effectiveness and core processes are directly affected by poor quality IT deliverables. There is failure of IT initiatives which were intended to bring innovation to the enterprise and either failed to achieve their promise or their deadlines were not met or the costs were higher than expected and/or quality and efficiency were lower than anticipated. The technology that has been purchased frequently becomes inadequate for the organisation or becomes obsolete too quickly and its support poor (IT Governance Institute, 2003).

Senior management and the board have often been disillusioned by the lack of returns from past technology investments (Changepoint Corporation, 2004). The following quotes illustrate some of the frustration felt:

“IT has been the longest running disappointment in business in the last 30 years!” - Jack Welch, Chairman, General Electric, World Economic Forum, Davos, 1997 (Thorpe, 1997).

“Technology can help fulfill a visionary dream, but often its use is closer to a sobering nightmare!” - Vesa Vaino, CEO Merita Bank, SIBOS, Helsinki, 1998 (Schirmbrand, 1998).

“I am writing a book on the history of information technology in order to better understand why it is such a mess!” - Philippe Corniou, CIO, Renault, IT Governance Forum, Paris, 2001 (Schirmbrand, 1998).

4.3.4 IT has not received the attention it deserves

Technology has greatly enabled the organisation whilst it has likewise become more critical. The failure of the technology, even briefly, can have a profound effect on the running and productivity of the organisation. Technology has changed over the last 20 years and permeated all facets of the organisation therefore information processing is no longer centralised. Businesses now ‘reside’ where the employees are and can move from office to office, or from city to city with the advent of personal computers, networking and laptops (Whitman & Mattord, 2004). IT requires more technical insight with this increase in organisational fluidity, as far as understanding how it can enable the organisation, create risks and give rise to opportunities than do other
disciplines of an organisation. IT has, traditionally, been treated as an entity separate to the business because the board and senior management find IT complex, especially in the extended organisation operating in a networked economy. This has meant they have tended to shy away from it, leaving it in the hands of the IT department. This is no longer appropriate in the current information critical society.

4.3.5 IT involves huge investments and large risks

Organisations depend on IT to facilitate nearly all their daily business transactions and the need for greater capacity and speed is ever increasing. This has resulted in the rapid escalation of IT investment in new technologies to meet this ever increasing need to improve on the productivity of the company and, in turn, the competitive edge. This is one of the reasons that dictate that the board becomes involved in providing relevant, adequate and effective IT governance. In 2003, 55% of the capital investment of an average company went into information technology (Alter, 2004). Companies are increasingly being challenged to manage and govern IT more effectively and efficiently as IT becomes more critical to organisations and more pervasive, ensuring that they balance the opportunities of new technology with the risks that it inherently carries.

The following are some examples of IT disasters that have cost companies large amounts of money (ComputerWorld, 2002):

- 1992: A conglomerate project, called Confirm, with AMR Corp., Budget Rent A Car Corp., Hilton Hotels Corp. and Marriott International Inc. costing $125 million in development, collapsed when it became clear that the project was two years behind its deadline. Mismanagement and the lack of goals were cited;

- 1994: Greyhound Lines Inc. built a new reservation and bus-dispatch system, called Trips, costing $6 million. It failed miserably when installed, crashed routinely, and resulted in the CEO and CFO resigning;

- 1996: A giant agriculture co-operative, Tri Valley Growers, bought $6 million worth of ERP software and services. None of the software
worked as promised, some could not even be installed on their DEC Alpha hardware. They finally filed for bankruptcy in July 1996;

- 1997: A new order-entry system cost Snap-On Inc. $50 million in lost sales as the franchisees could not operate the new system, despite three years of design and implementation.

These disasters indicate a possible lack of effective and efficient IT governance and illustrate the dire consequences of not balancing investment and risks appropriately. The board needs to oversee IT effectively to reduce the negative impact these types of disasters can have on the value and reputation of the enterprise.

All information technology investment decisions, either for or against, can expose an organisation to significant financial, operational and competitive risk. These risks need to be assessed in alignment with the strategic planning and risk management framework of the enterprise ensuring that the best decision is reached to enhance its competitive advantage and deliver measurable value (IT Governance Ltd, 2004b).

During the last few years there have been many disasters of large information technology investments, such as, major ERP systems initiatives that were never completed, e-business initiatives that were ill-conceived or poorly executed and new systems developed that were never used effectively. Other companies, in contrast, have been receiving above industry average returns from their IT investments year after year. These companies make better IT decisions and they make them more consistently. The reason is better information technology governance because they have the right people making IT-related decisions more effectively than their competitors (Weill & Woodham, 2002). A brief discussion on the objectives and purposes of IT governance will show the importance of having the right people making the more effective decisions to ensure that the expectations for IT are met and the IT risks are mitigated.

4.4 Objectives and Purposes of IT Governance

The IT Governance Institute (2003) states that “the overall objective of IT governance, ... is to understand the issues, and the strategic importance
of IT, so that the enterprise can sustain its operations and implement the strategies required, to extend its activities into the future.” IT governance needs to ensure that the expectations for IT are met and that IT risks are mitigated.

The board is not expected to consist of technological experts, but they need to ensure that they are asking the right questions of the right people, at the right time, to ensure that their current organisational situation can be sustained and their future expectations can be fully met, while ensuring that their risks are being managed efficiently (Trites, 2004).

The main purpose of IT governance is to direct and control IT projects ensuring that the performance of IT meets the strategies and goals laid down by the board and that performance is measured to ensure compliance. The use of IT needs to enable the company by exploiting the opportunities and maximising the benefits through the responsible use of its resources (IT Governance Institute, 2003). The board and senior management need to take a thoughtful and deliberate approach to IT governance, understanding that another of its purposes is to encourage desirable behaviours in the use of IT (Weill & Broadbent, 2003).

Effective IT governance encourages and leverages the ingenuity of all the users of IT within the organisation, not just its leaders, while still ensuring compliance with the its overall vision and principles. Peter Weill, Director of the Massachusetts Institute of Technology, believes that “effective IT governance is the single most important predictor of getting value from IT.” (Weill & Woodham, 2002).

Some of the elements that constitute effective information technology governance will now be examined.

4.5 The Elements of Information Technology Governance

After an extensive literature study on the definitions of IT governance, (IT Governance Institute, 2003), (Changepoint Corporation, 2004), (IT Governance Institute, 2003), (Exler, 2003), the following common elements were identified (not claimed to be all inclusive). These include:
• The responsibility of the board of directors;

• It entails Risk Management and Transparency;

• The need to direct and control IT investment, opportunity, benefits and risks;

• The alignment of IT strategy with business strategy;

• The assignment of accountability and responsibility;

• The sustainment of current status and the preparation for the future;

• The maintenance of IT internal controls for financial reporting and disclosure.

These elements will be examined in more detail obtaining a clearer picture of what IT governance actually entails.

4.5.1 The Responsibility of the Board of Directors

The first element implies that IT governance rests on the shoulders of the board of directors. The IT Governance Institute (2003) states that IT Governance is the responsibility of the board of directors and executive management and needs to be an integral part of its overall corporate governance structure and not seen as an isolated discipline.

Ron Exler, an analyst with Robert Francis Group states that “Corporate governance and IT governance are now intimately intertwined.” (Change-point Corporation, 2004).

A main objective of the board is to protect shareholder value. Change-point (2004) maintain that “the underlying responsibility of the board is to oversee and advise management and to represent the interests of the shareholders.” Directors need to oversee the investment of shareholder and a large portion of this goes into IT investments. Increasingly, there is an educated and assertive set of stakeholders who are concerned with the sound management of their interests and, according to McKinsey’s Investors Opinion Survey of June 2000, are prepared to pay a premium of more than 20% for the shares of enterprises that have shown to have good governance practices in place, which includes IT governance (King Committee on Corporate Governance, 2002).
4.5. THE ELEMENTS OF INFORMATION TECHNOLOGY GOVERNANCE

This is further borne out by the following statement by Robert S Roussey, Professor at University of Southern California, where he states that “IT governance is the term used to describe how those persons entrusted with governance of an entity will consider IT in their supervision, monitoring, control and direction of the entity.” (IT Governance Institute, 2003).

The application of IT within the organisation has an immense impact on whether that organisation will attain its vision, mission or strategic goals. All these statements indicate that IT governance should not be left to the IT department, but needs to be embraced by the board and senior management, preferably within the corporate information division as proposed in chapter three.

4.5.2 It Entails Risk Management and Transparency

Another element in IT governance definitions is the ensuring of Risk Management and Transparency. Moulton (2004) states that the board has a duty to satisfy their stakeholders that all risks, relating to IT, are being effectively managed and governed.

The new regulatory environment has intensified the governance and risk management demands on CEOs, Chief Financial Officers (CFOs) and their boards of directors. Part of IT governance includes ensuring compliance to new legislation, but it must not stop there. IT governance is required to create a climate of trust and confidence through oversight. Governance, in general, deals with the core aspects of the business and how their content can be made transparent for stakeholders of the corporation. The term *transparent* refers to the ability of the board, investors and stakeholders to understand the key drivers, metrics and risks that exist for an organisation and how the organisation is faring in meeting key metrics over time (Loyd, 2004). This applies equally to the governance of IT and its risks. A climate of trust and confidence is achievable through transparency. There arises a greater need for corporate transparency and accountability and companies must, for the first time, make themselves clearly visible to all stakeholders and society with regard to all aspects of governance especially their risks. Greater transparency engenders more confidence and likewise, a lack of transparency could result in a lack of trust in a company (Institute of Internal Auditors, 2000b). The building of transparency into IT governance increases confidence in the
risk management of a company, because their processes and procedures are clearly visible and risks are not being hidden.

### 4.5.3 The need to direct and control IT investment, opportunity, benefits and risk

Two of the main functions of corporate governance are directing and controlling, and these need equally to be found in IT governance. This is borne out by the following statement: information technology governance is a structure of relationships and processes, which include directing and controlling the organisation. These directing and controlling functions are especially important in the areas of IT investment, opportunities, benefits and risk. IT governance needs to facilitate the achievement of the goals of the organisation by adding value, while balancing risk versus return for IT and its processes (Exler, 2003). The large amount of money spent on IT, the strategic opportunities and the risks which these investments present, dictate board-level risk management and governance activities for IT (Changepoint Corporation, 2004).

### 4.5.4 The alignment of IT strategy with business strategy

A further element of IT governance is the alignment of IT strategy with business strategy. The IT Governance Institute (2003) states that information technology governance is fundamentally about two things: The delivery by IT of value to the business and the mitigation of IT risks. The delivery by IT of value is driven by the strategic alignment of IT with the business whilst the mitigation of IT risks is driven by ensuring that accountability is embedded into the organisation. Both require to be supported by adequate resources and to be measured ensuring that the required results are obtained (IT Governance Institute, 2003).

Information technology governance has further been defined as the disciplined management of IT investment decisions and performance monitoring. This includes the processes that govern decision-making around investment decisions, client relationships, project management and other important operational areas (Hoffman, 2003). IT governance includes the monitoring of
IT performance ensuring that IT adds value to the organisation; that its strategy is aligned with the business strategies; and that this is not only due to the consequences of lack of compliance (Weill & Woodham, 2002).

Information technology governance is required to ensure that IT investment decisions are not just merely in line with the business strategic objectives of the organisation, but that they are derived from an IT strategy that, itself, is derived from an appropriate analysis of these organisational business objectives. This leads to investment decisions that enhance competitive advantage, improve business processes and contribute to growth that both protects and enhances shareholder value (IT Governance Ltd, 2004b).

4.5.5 The assignment of accountability and responsibility

Peter Weill, Senior Research Scientist and Director CISR, MIT Sloan School, maintains that IT governance is defined as “specifying the decision rights and accountability framework to encourage desirable behaviour in the use of IT”. He continues to say that IT governance needs to apply principles to IT management that are similar to those for financial governance. Companies need to encourage particular desirable behaviours that exploit and reinforce the human, systems and intangible assets that comprise their core competency to achieve their goals. He cites the example of companies that he studied, where the business objective of “sharing and reuse” was achieved by encouraging the desirable behaviour of “look within the company first”. This was evaluated with a targeted measure of performance, for example, return on assets (ROA). The IT governance structure should encourage desirable behaviours and incorporate all major aspects of IT use, which include IT principles, investment and prioritization, planning, infrastructure, applications development, architecture, payoff measurement and accountability (Weill & Woodham, 2002).

There can be no efficient, adequate IT governance without the co-operation of the entire organisation. The goals and strategies of the board need to be filtered through the entire company. Adequate means of measurement and monitoring should be made available to ensure that compliance is being achieved. All levels of the company need to apply the same principles
CHAPTER 4. THE GOVERNANCE OF INFORMATION TECHNOLOGY

of setting objectives, providing and receiving direction, and providing and evaluating performance measurements to have effective IT governance in the organisation (IT Governance Institute, 2003).

It is important to note that successful IT governance models strongly embed the culture, processes and values of an enterprise and that proper governance requires accountability, measurement, direction and control (Exler, 2003).

4.5.6 The sustainment of current status and preparation for the future

IT governance needs to sustain the current operation and prepare for the future. It needs to oversee the creation and the implementation of a set of policies and procedures enabling the IT resources of the organisation to realise their business goals.

The board, according to Richard Nolan, a Harvard Business School Professor, needs to be aware of emerging technologies, operations, architecture, and strategic potential and jeopardy. The board is wary of surprises and finding that “their legacy system is a ticking time bomb which will blow in the next six months, and that they will have to invest $300 million to save their systems, is the kind of surprise that blows out earnings and just ought not to happen” (Alter, 2004).

The board cannot be expected to become experts in technology or current IT trends, but they must ensure there are processes in place for the organisation to monitor its current situation, and consider new technological developments for their future strategic initiatives (Trites, 2004). The board needs to understand the IT components of their IT strategy how these components are intended to sustain and drive the business value of the organisation. The board should take steps to identify all the critical dependencies and inter-relationships between the components of its IT infrastructure and ensure that it is sufficiently mature to both sustain and grow the organisation (IT Governance Ltd, 2004b).

The management and allocation of resources is also an important issue in sustaining the current status and preparing for the future of the enterprise because it includes optimizing knowledge and infrastructure. The manage-
ment and allocation of resources includes people, applications, technology, facilities and data (IT Governance Institute, 2003). Decisions on dealing with information risks are, on occasions, made by competent IT managers, who are not involved in, or responsible for, the strategic management of IT. This can result in the purchase and deployment of information security technology that is inappropriate in the light of the real risks faced by the organisation (Business Software Alliance, 2003).

“The goal of resource management is to optimise the utilisation of IT assets, lower the total cost of ownership, improve IT investment decisions and unlock the promise of computing by making knowledge resources more productive” (InfoSec, 2003). Good resource management and allocation is a vital aspect of good IT governance.

4.5.7 The maintenance of IT internal controls for financial reporting and disclosure

Much attention has been focused on financial reporting and disclosure and it is generally conceded that the reliability of financial reporting depends to a large extent on a well-controlled IT environment. Therefore, there is the need, within an organisation, to include the oversight of the implementation of IT internal controls over financial reporting, within the IT governance structure to provide reasonable assurance regarding the reliability of financial reporting. The Sarbanes-Oxley Act of 2002 was created to improve corporate responsibility and to restore investor confidence in United States public markets, which had been damaged by business scandals and lapses in corporate governance. This Act aimed to improve corporate governance through measures that would strengthen internal checks and balances and, ultimately, strengthen corporate accountability (IT Governance Institute, 2004).

The implementation of a strong internal control program within IT can help enhance IT governance. It can further enhance the understanding of IT among executives and create an environment where better business decisions are made with higher-quality and more timely information. A strong internal control program can help enable the aligning of project initiatives with business requirements. It can prevent the loss of intellectual assets and the possibility of a system breach and the gaining of a competitive advantage.
through more efficient and effective operations. It can optimise operations with an integrated approach to security, availability and processing integrity and lastly, enhance risk management competencies and prioritisation of initiatives (IT Governance Institute, 2004).

In the current environment, “financial reporting processes are driven by IT systems” (IT Governance Institute, 2004). Therefore, IT plays a critical role in the operations of an organisation and in internal controls and reporting information. At the same time it has fiduciary implications because of the electronic formation of contracts, the integrity of electronic communications and the retention of records. Directors need to ensure that their organisation has the necessary skills, with respect to IT, in place to discharge their responsibility for internal controls. IT can improve reporting and transparency, but the directors need to be aware of the blurring of organisational barriers which has arisen as a consequence of e-business (King Report, 2001).

A clearly defined IT governance program needs to be implemented for IT governance to achieve its objectives. This program is discussed next to examine the steps required to achieve this objective and what the involvement of the board should be.

4.6 Proposed IT Governance Program

An IT governance program should be thoughtfully designed to encourage desirable organisational behaviours, but too often business and IT governance just happens. The defining of desirable behaviours takes time, effort and focus. It is important that the board realises that an effective IT governance program is not a “one size fits all”. It differs due to the desired business objectives and the behaviour sought (Weill & Broadbent, 2003).

There are three main reasons stated for the failure of the implementation of an IT governance process, namely: the inadequate participation, ownership and leadership by the board and senior management; a lack of clearly articulated goals with respect to IT strategy and lastly, a lack of clearly defined governance process (Gerrard, 2004). All these issues need to be addressed when implementing an IT governance program.

The process of designing an information technology governance program starts with the setting of clear objectives and principles for IT, defining
the role that IT will play within and across the organisation and providing its initial direction. These principles are defined in the context of business strategy. Next, the roles and responsibilities of the different levels of the organisation need to be assigned (Gerrard, 2004). A continuous cycle for measuring performance, comparing objectives is established and this results in the redirection of activities where necessary and a change to objectives where appropriate. The setting of objectives and principles is primarily the responsibility of the board and requires senior management buy-in and sponsorship. This, in turn, provides the oversight, strategic direction and support for the process. The measuring of performance is the responsibility of management and it is important that the objectives and measures are developed in tandem to ensure the objectives are achievable and the measures represent the objectives correctly (IT Governance Institute, 2003).

An IT governance program needs to be consistently and continuously implemented and managed.

There are various steps the board should take with regards to an IT governance program. The key steps include (IT Governance Ltd, 2004a):

- The need to recognise, at board level, that IT governance is a “must have”;
- The need to make the CIO, who should be a board member (as proposed in Chapter Three), responsible for IT governance and adopt an appropriate IT governance framework;
- The need to carry out a high level Risk Assessment, within the context of the broader approach to risk by the organisation;
- The ability to act on the outcomes of that assessment;
- The ability to derive an information strategy from an analysis of strategic objectives and use this to contextualise and/or derive IT investment options;
- The ability to implement a risk and value based approach to making and monitoring these decisions.
The effort required to achieve “full-cycle” IT governance is difficult, but believing that any project can succeed provided there are enough business sponsors, expertise and money is incorrect. “Business sponsorship is a weak substitute for leadership. Buying in from management and board motivates business leaders to assign their top talent, establish baseline measurement systems, manage risks and manage project scope, and see the changes through.” (Cramm, 2004). A “full-cycle” governance process encourages business leaders to ensure project accountability is filtered throughout their companies rather than leaving accountability to the IT managers (Cramm, 2004).

4.7 Conclusion

The formation of separate executive responsibilities within the corporate governance structure, charged with a specific responsibility for governing the information asset was proposed in Chapter Three. It was further proposed that information technology governance forms one of two components of corporate information governance. This chapter has confined itself to an analysis of the component, information technology governance, and what its proper place should be in the corporate governance culture.

A clearer understanding of what information technology is, what its importance has been as a governance issue and what many noteworthy persons and institutions believe information technology governance should become, to reduce the incidence of corporate failures and losses due to poor information governance, has been described.

Information technology governance has been validated as a top level corporate governance issue and the following chapter applies itself to a study of the second component of corporate information governance, namely the governance of information security. The aspects of information security and its governance will be examined. The importance of information technology governance to an organisation was detailed in this chapter and the following chapter will highlight the importance of information security governance to an organisation.
Chapter 5
The Governance of Information Security
5.1 Introduction

The governance of information security is an important issue to be considered by all corporate boards. Data and information can be equated to an organisation’s “life blood” and compromising this “life blood”, could “kill” the organisation (von Solms & von Solms, 2005). The board and senior executives must have a clear understanding of what to expect from the information security program of the enterprise to exercise effective organisational and information security governance (IT Governance Institute, 2001). In this regard, the famous motto of Lord Baden Powell “Be Prepared” is particularly relevant because the board needs to formulate an information security program designed around specific issues including risk. Roles and responsibilities require allocation and a sound implementation plan requires establishment.

The importance of the governance of information technology was examined in the previous chapter. The different aspects of information technology were discussed, illustrating how technology has evolved, what its purpose is and what its expectations are. The importance of information technology was highlighted from the perspective of the board and the governance of information technology was shown to be a vital function of the board and senior management.

This chapter examines the second identified component of corporate information governance, namely the governance of information security. Different aspects of information security will be discussed providing a background to information security and what it entails. This chapter focuses on information security governance, defining it, indicating the important pillars on which it stands and will demonstrate that, like information technology governance, the information security governance function is a direct responsibility of the board and executive management and that there can be serious personal and legal consequences should this governance function is ignored. Lastly, a process is proposed to improve the function of information security governance.

5.2 Information Security

Technology has changed over the last twenty years and permeated all facets of the organisation and information processing is no longer centralised. There
has been an increase in business fluidity with the advent of personal computers and laptops and consequently, the concept of computer security has been replaced by the concept information security. The issues covered by information security are broader and include more than the protection of data. It includes the protection of human resources and can no longer be considered the sole responsibility of a small, dedicated group of people within the organisation, but rather as the responsibility of every employee, manager and the board (Whitman & Mattord, 2004). The current economy depends on a secure flow of information within and across an organisation, which indicates that information security should be considered an issue of vital importance.

5.2.1 Definition of Information Security

It would be wise first to look at an each word separately when trying to define information security. Information was defined in Chapter Two as “data endowed with relevance and purpose. Converting data into information thus requires knowledge. Knowledge, by definition, is specialised” (Frenzel, 1992). Generally, security is defined as the quality or state of being secure - to be free from danger (Merriam-Webster, 2002). Therefore, information security can be defined as the protection (from danger) of information and its critical elements through the systems and hardware that use, store, and transmit that information (Whitman & Mattord, 2003). Information security should be more than merely freedom from danger; it needs to include freedom from undesirable events, such as malicious and accidental misuse. A measure of organisational security can be measured by the degree to which a system resists intrusions by outsiders and misuse by insiders (Anderson, 2003).

Information security, according to Ernst and Young (2005), deals with the protection of information in its electronic form and in its paper-based forms. It needs to ensure this protection throughout the entire information life-cycle for capture, processing, use, storage and destruction. Therefore, for information security to be truly effective, the dimensions which need to be addressed must include people, processes and technology.
5.2.2 Characteristics of Information Security

It is important to be familiar with the key characteristics of information, which makes it valuable to an organisation to better understand what is involved in information security. These include confidentiality, integrity, availability, privacy, identification, authentication, authorization and accountability (Whitman & Mattord, 2003). Each key characteristic will be briefly discussed.

1. Confidentiality

Confidentiality of information is defined as ensuring that information of a specific classification is not distributed to people outside the category for which it is classified. It ensures that only those people who have the correct rights and privileges will be able to access that information. The category for which the information is classified could be a specific organisation, department or an individual. Confidentiality is breached when confidential information is accessed by unauthorised parties or the information is disclosed by employees without authorisation.

Confidentiality can be protected by, inter alia (Whitman & Mattord, 2003):

- The classification of information;
- The secure storage of documents;
- Ensuring the application of general security policies;
- Educating information custodians and end users;
- Using cryptography.

It is of vital importance that the personal information of employees, customers or patients is kept confidential. Legislation, such as the Health Insurance Portability and Accountability Act (HIPPA) of 1996, focuses specifically on the health industry to ensure the portability, confidentiality, privacy and security of medical information for individuals (OpenService, Inc, 2004). HIPAA requires that organisations prevent unauthorised access, alteration, deletion, and transmission of electronically stored and transmitted
5.2. INFORMATION SECURITY

protected health information because electronic transmission is open to violation. CEOs, CIOs and/or auditors face penalties of $100 to $25000 per person, per year, per incident of unintentional disclosure, or ten years in jail for wrongful disclosure of medical information, or both (Sophos, Inc, 2004). It is evident that there are severe consequences with regard to lack of confidentiality and privacy of information within an organisation.

Disclosure of confidential information can be either deliberate or unintentional, for example, confidential information could be mistakenly e-mailed to someone outside the organisation rather than inside the organisation; or a confidential document is discarded and not destroyed; or someone could successfully hack into an internal database and steal all the customer credit card information.

2. Integrity

Integrity is concerned with the quality, validity and reliability of the information. Integrity is not concerned with the origin of the data, but whether it has been modified since its creation (Schneier, 2000). The integrity of information is compromised when it is exposed to corruption, damage, destruction or other disruptions to its authentic state. Corruption of the information can occur while it is being entered, stored or transmitted (Whitman & Mattord, 2003).

The corruption of a file could be due to computer viruses and worms, or due to faulty programming, or even noise on the transmission channel or media. The prevention of internal and external threats to the integrity of information uses error control techniques such as redundancy bits and check bits, algorithms, and hash values. Information that is unable to have its integrity verified, is of little or no use to an organisation.

3. Availability

Availability is concerned with enabling authorised user access to information, without being hindered or obstructed, and in a usable format. The user may be an individual or a computer system (Whitman & Mattord, 2003). This information must be available in a timely basis so that strategic and business decisions can be effected when necessary. Denial of service attacks
by outside perpetrators is also be a serious threat to the availability of information of an organisation. Lack of availability can harm the organisation as opportunities may be lost, deadlines missed, commitments defaulted or work progress may be impaired. Should information be exactly what is needed to meet organisational requirements, if it is not available timeously, it becomes useless (Bruce & Dempsey, 1997).

4. Privacy

Privacy is concerned with ensuring that the information that is collected, used and stored by an organisation, is only used for the purposes stated to the data owner at such time it was collected. Many companies collect and sell personal information as a commodity. It is now possible to collect and combine information about individuals from separate sources and companies can produce detailed databases whose data might be used in ways not agreed to, or even communicated to, the original data owner (Whitman & Mattord, 2003).

5. Identification

Identification within an information system is the ability to recognise individual users. Identification is the first step in gaining access to secured material and serves as the foundation for subsequent authentication and authorisation processes. Identification and authentication processes are essential to establish the level of access or authorisation that an individual can be granted by a database administrator. A user name or another form of identifier are examples of means of identification (Whitman & Mattord, 2003).

6. Authentication

Authentication is defined by ISO/IEC Technical Report 13335-1 (1996) as “the property that ensures that the identity of a subject or resource is the one claimed. Authenticity applies to entities such as users, processes, systems and information.” Authentication occurs when a control provides proof that a user possesses the identity that he or she claims. Examples of authentication processes include the use of cryptography certificates to establish Secure Sockets Layer (SSL) connections, or the use of cryptographic hard-
ware tokens like SecurID cards to confirm the identity of a user (Whitman & Mattord, 2003).

7. Authorization

Authorisation is the process that provides assurance that the user (whether a person or computer) has been specifically and explicitly authorized by the proper authority to access, update or delete the contents of an information asset. This generally happens after the identity of the user has been authenticated. An example of this control is the activation and use of access control lists and authorization groups in a networking environment. It is used, in a database authorization scheme, to verify that the user of the application is authorized for specific functions such as read, write, create and delete (Whitman & Mattord, 2003).

8. Accountability

The characteristic of accountability exists when the assurance is provided by a control that every activity undertaken can be attributed to a named person or automated process. Audit logs can be used to track user activity on an information system in order to provide accountability (Whitman & Mattord, 2003).

Each of the above characteristic plays an important part in the process of information security and need to be in place to ensure that the information of an organisation is protected and secure. A board that assures itself that all eight of the above characteristics are included in their information security program has taken a positive step in fulfilling their due care and due diligence. The provision of accurate and valid information at the right time makes the difference between profit and loss or success and failure. Shareholders and others need to receive comprehensive financial reports, which are accurate to be informed participants within the governance structure. Good information security requires that these reports have integrity, and that their disclosure is timely and balanced (Corporate Governance Task Force, 2003).
5.2.3 The Importance of Information Security

Information security is important for the following reasons (National Cyber Security Partnership Governance Task Force, 2004):

- Significant damage to organisations has occurred due to breaches of information security;

- There has been a dramatic increase in intrusions, worms and viruses over the last few years;

- The risks and costs involved, due to loss of business continuity, can be considerable;

- There is a serious threat of financial and criminal liability for the organisation if it is found to be non-compliant with relevant legislation.

Can the information assets of an enterprise ever be free from danger? This is generally not the case, as is illustrated by the following examples and statistics of security breaches.

The Department of Trade and Industry’s 2004 Information Security Breaches Survey in the United Kingdom reflected that over 70% of organisations reported that they had suffered a security breach in the previous year (Department of Trade and Industry, UK, 2004). The published FBI statistics forecast that a company has a 90% chance of being a victim to an information security breach over the next year (Bergamo, 2005). These are very frightening statistics and the board needs to take cognizance of them by ensuring that an adequate plan of action is implemented to prevent their company from becoming another victim because the consequences could be devastating.

The government of the United States of America has established legislation and regulations with regard to information security. Some of these laws address information security directly, while others address it indirectly through issues such as financial governance, privacy or reporting requirements. It is advantageous to examine any legislation pertaining to this subject to see how it affects the security of the organisation.

Laws and Regulations concerning Information Security

The following legislation and regulations apply directly or indirectly to information security and carry with them civil and/or criminal penalties.
Table 5.1 was published by the Business Software Alliance and clearly states the legislation, who is affected, what security provisions are covered and the associated penalties (Business Software Alliance, 2003). There are many other laws in different countries, but these listed in Table 5.1 are examples indicating their affect on information security.

<table>
<thead>
<tr>
<th>Legislation</th>
<th>Who is affected?</th>
<th>What do the security provisions cover?</th>
<th>What are the penalties?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sarbanes-Oxley Act of 2002</td>
<td>All public companies subject to US security laws</td>
<td>Internal controls and financial disclosures</td>
<td>Criminal and civil penalties</td>
</tr>
<tr>
<td>Gramm-Leach_Biley Act of 1999</td>
<td>Financial institutions</td>
<td>Security of customer records</td>
<td>Criminal and civil penalties</td>
</tr>
<tr>
<td>Health Insurance Privacy and Accountability Act of 2005</td>
<td>Health plans, health care clearinghouses, and health care providers</td>
<td>Personal health information in electronic form</td>
<td>Civil fines and criminal penalties</td>
</tr>
<tr>
<td>California Database Security Breach Information Act</td>
<td>State agencies, persons and businesses that conduct business in the State of California</td>
<td>Reporting of breaches of unencrypted personal information</td>
<td>Civil fines and private right of action</td>
</tr>
</tbody>
</table>

Table 5.1: Impact of Recent Information Security Legislation

These laws and regulations detailed in Table 5.1, apply to the United States of America, South Africa has the Electronic Communications and Transactions Act of 2002 (ECT Act) that equally applies to information security. It affects all people and businesses in South Africa that use electronic information. The security provisions covered include security of customer records, retention of records, encryption of sensitive data, hacking and intrusion software and the security of payment methods for e-Commerce
businesses. There are both criminal and civil penalties. Other examples of legislation in South Africa governing information include the Promotion of Access to Information Act and the Regulation of Inception of Communications Act. Affected entities include all corporate bodies and other companies which hold information including individuals. Non-compliance carries both civil and criminal penalties.

It is important for the board to be aware of all legislation, South African and international, as many organisations transact business with companies, both locally and in other countries.

**Potential Consequences of Information Security Breaches**

Information is being shared increasingly with the use of e-commerce and information exchanges on the Internet. It is automatic to protect the house and personal belongings of an individual against unauthorised entry, theft and damage, the information asset of an organisation require the same protection. The criticality of information security to an organisation is highlighted by the following potential consequences due to security breaches (Gordon and Glickson LLC., 1998):

- A loss of consumer goodwill - It was noted in a survey that fewer than four out of ten consumers felt that most businesses had protected their personal information ‘properly and confidentially’. Questionable privacy practices within an organisation can chase customers away;

- A loss of sensitive or critical organisational information - which could directly affect its competitiveness and cash flow and damage its reputation. It takes many years to establish a good reputation and image as a trustworthy and reliable business, but this can be destroyed within a matter of hours by a security breach;

- A violation of legislation - Table 5.1 indicates some of the legislation that is applicable to information security and the penalties for non-compliance;

- The corruption of computer systems - inadequate information security can lead to the corruption of the computer systems of an organisation
through the use of ‘trojan horses’ and other means, which can seriously affect its ability to continue business.

Price WaterHouse & Coopers (2002), in their 2002 Information Security Breaches Survey, highlight the lack of support for information security because security is generally treated by the board as a cost overhead rather than an investment. They furthermore, state that only 27% of organisations in the United Kingdom spend more than 1% of their information technology budget on protecting their information and only 5% of organisations spend more than 10% of their IT budget on information security (PriceWaterhouseCoopers, 2002). These statistics indicate a serious lack of focus on information security by the boards of companies and this lack needs to be rectified.

The Companies Act No 61 of 1973, section 424, states that a director and even the CIO, may be personally liable for unlimited damages should the failure to identify and manage risks be classified as reckless management on the part of the company by the Law courts. Thus, should senior management be aware of a specific risk and chooses to ignore it (called the *ignorantia legis neminem excusat* principle) and it results in serious losses, criminal liability could occur (Hinde, 2003).

### 5.2.4 Summary

There is an increase in the dependence on information in the current economy and information security can no longer be ignored. The security of the information of an organisation can mean the difference between its success or failure. Traditionally, information security has been about ensuring the confidentiality, integrity and availability of the information asset, but this needs to be extended to include the following issues - privacy, identification, authentication, authorisation and accountability amongst others. All these characteristics need to be implemented effectively within the organisation to ensure that all aspects of the information asset are adequately protected.

The *hands on* function of ensuring information security is a management one. It ensures that the strategies, goals and objectives as *set by the board* are implemented throughout the organisation. All the different business unit heads within the organisation have a role in the management of information
security and for it to be effectively implemented, it needs their commitment.

This presents the next question - what is the function of the board in relation to information security?

5.3 Information Security as a Governance Issue

The Corporate Governance Task Force (2004) state that for information security to be effective, it needs to be incorporated into the corporate governance policy of the organisation. Generally, information security is viewed as a technical issue; however, it should be considered a governance challenge that involves risk management, reporting, and accountability. Senior management and the board need to ensure that they are not merely interested in being aware of and managing the financial risks, but need to govern the business information risks to ensure the survival of the organisation. Strategic decisions, in this information-driven age, are made based on business information and therefore, the board and senior management must be aware of and held accountable for managing the risks that could compromise the security of the information of the organisation (National Cyber Security Partnership Governance Task Force, 2004).

The oversight of information security can no longer be left to the lower levels of management. Its importance as a business responsibility dictates that accountability for this function be escalated to board level as a governance issue.

von Solms, B. and von Solms, R (2005) in their paper From Information Security to .... Business Security?; variously quote for the importance of the escalation of responsibility and accountability for information security to board level:

“Corporate Governance consists of the set of policies and internal controls by which organisations, irrespective of size or form, are directed and managed. Information security governance is a subset of organisations' overall governance program” (National Cyber Security Partnership Governance Task Force, 2004);
“...boards of directors will increasingly be expected to make information security an intrinsic part of governance, preferably integrated with the process they have in place to govern IT” (IT Governance Institute, 2001);

“However, for information security to be properly addressed, greater involvement of boards of directors, executive management and business process owners is required” (IT Governance Institute, 2001);

“An information security program is a risk mitigation method like other control and governance actions and should therefore clearly fit into overall enterprise governance” (IT Governance Institute, 2001).

All the above quotes directly place the responsibility of information security governance in the domain of the board and senior executives. Thus, under the corporate information governance responsibilities proposed in Chapter Three, the responsibility for information security governance lies equally on the shoulders of the CIO, who should, ideally, have a seat on the board of directors.

5.3.1 Information Security Governance Defined

The National Cyber Security Partnership Governance Task Force (2004) state that information security governance is a “subset of corporate governance” relating to the security of the information assets of an organisation. This statement is extended and information security governance should include:

1. The setting of strategies, objectives and policies for information security by the board;

2. The setting of the risk appetite of the organisation;

3. The assignment of a roles and a responsibility structure;

4. The setting of the ethical standards of the organisation;

5. The oversight for the resource investment for information security;
6. The oversight for compliance with applicable legislation and regulations;

7. The oversight of investor relations and communications activity, including Transparency.

Rolf Moulton et al. (2003) define information security governance as “the establishment and maintenance of the control environment to manage (or oversee) the risks relating to the confidentiality, integrity and availability of information and its supporting processes and systems.”

Information security governance has been defined as a ‘subset of corporate governance’ and it should include the following responsibilities.

1. The setting of strategies, objectives and policies for information security by the board

The oversight of information security is critical to an organisation due to many factors, one being the increasing dependence on information and the systems and communications that deliver it. The fragile state of information security demands that the board ensures that the procedures and processes implemented to ensure that data and information are not compromised and remain secure (National Cyber Security Partnership Governance Task Force, 2004). Information security is a strategic, business issue that will fail to realise any meaningful business value should the board and senior executives not direct the development and deployment of the information security strategy (Ernst and Young, 2005).

The dependence of most organisations on information has grown so rapidly that a disruption in the flow of information has become a component when calculating operational risk. This was highlighted by the September 11, 2001 attack on the World Trade Centre as described in the previous chapter (Sungard Availability Services, 2004).

It is critical that the board set strategies, objectives and policies with regard to the oversight of information security. It has a responsibility to maintain the financial and material health of the organisation by setting the proper direction for information security and the security culture required to demonstrate due care and due diligence. Due care is defined as the acceptance and implementation of recognised and reasonable best practices, while
due diligence is defined as the amount of care that a prudent party would exercise to avoid harming another body (Bergamo, 2005). Information security cannot be enforced within an organisation without a mandate. A corporate information security policy is the organisational mandate and contains a series of baseline information counter measures crucial to the organisation (von Solms, 2001b).

Corporate information security policies are direction-giving documents that define the concepts of information security and require the commitment and support of the board and senior executives to ensure success. They define the role that information security plays in reaching and supporting the vision and mission of the organisation. They are a vital part of its strategy for achieving information security (Hone & Eloff, 2002). It is critical that the board ensures that its corporate information security policy is aligned with its business strategies. All stakeholders need to be given an opportunity to input into this document ensuring that there is a general ownership and therefore, a commitment to information security from board level right throughout the organisation.

It is wise for the board to decide whether a code of best practice should be implemented within the organisation to ensure that all aspects of information security are covered by the organisation. Basie von Solms (2001) maintains that a code of best practice “can be seen as the Information Security “Wheel”, invented, tried and tested by other people.” The implementation of a recognised code of best practice ensures that the organisation has the assurance that they are equal with international best practices. A code of best practice provides the organisation with a reference framework ensuring that all information security aspects are covered and spares the organisation the effort of reinventing the Information Security “Wheel”. Examples of good best practice documents for use by an organisation to set up their information security, include the ISO 17799, ISO 13335, and the Guidelines for the Security of Information Systems document by the Organisation for Economic Cooperation and Development (OECD). These documents can be used to ensure that they are addressing most of their information security risks without necessarily going through a comprehensive risk analysis exercise (von Solms, 2001b). Therefore, it is critical that the board includes a directive in the corporate information security policy that a code of best
practice be implemented within the organisation.

A quality information security program starts and ends with quality corporate policies. The main aim of any policy is to influence and determine decisions and actions by specifying what behaviour is acceptable and unacceptable (Whitman & Mattord, 2003).

2. The setting of the risk appetite of the organisation

All businesses face risk, but if these risks are understood and managed properly, taking the right risks may produce a competitive advantage (Borland Software Corporation, 2005). Risk management is concerned with understanding the information or business risks and actively managing these risks to keep them within acceptable levels according to the risk appetite of the organisation (von Solms, 2003). Risk appetite defines the quantity and nature of risk that an organisation is willing to accept, as they evaluate the trade-offs between perfect security and unlimited accessibility (Whitman & Mattord, 2003).

The board needs to understand where their organisational risks lie enabling them to make well-informed decisions regarding the future of their company. The board needs to decide on a suitable risk strategy to follow with regard to risk acceptance, risk avoidance, risk transference and risk mitigation. The strategy the board chooses must satisfy their risk appetite (King Report, 2001). The board needs to oversee their policies and procedures and ensure they are implemented to protect the information asset. It is vital that information security measures are continuously audited and upgraded ensuring that the company protects its data and information from both internal and external threats.

The challenge for the board and senior management is to ensure that the information security solutions the organisation deploys are proportionate to the value of risk and in line with its strategic and operational goals (IT Governance Ltd, 2004b). John Lindquist, President and CEO, EWA Information and Infrastructure Technologies, Inc., stated that it is not enough just to protect the computer systems, but that it was important to protect the information assets and this involved risk management. Risk management, in turn, deals with people, processes and technology, which need to be integrated into the corporate information security policy as accepted by the
board to protect those assets. It is important that the board remember this process is a continuous one because risks can change over time and therefore, they need to be reassessed periodically (IT Governance Ltd, 2004b).

3. The assignment of roles and responsibility structure

One of the functions of the board and senior executives is the formation of a structure for the assignment of roles and responsibilities within the organisation. This allows the board to know who is accountable for what tasks and responsibilities. Accountability means that those individuals or groups of people in an organisation, who have the authority to make decisions, must equally have the responsibility and be accountable for their decisions and actions. Mechanisms allowing accountability provide investors with the means to query and assess the actions of the board and its committees. Responsibility pertains to the behaviour that allows for corrective action and for penalizing mismanagement. The board is accountable to the organisation and it must act responsively to and with responsibility towards all the stakeholders (King Report, 2001). Thus, management is responsible for information security and the board is accountable, as part of its duty of care, to provide effective information security oversight (Institute of Internal Auditors, 2001).

4. The setting of the ethical standards of the organisation

Ethics is an important issue with regard to information security governance because it sets the standard of ethical behaviour for the entire organisation. The standards of ethical behaviour of the organisation need to be structured in conjunction with its stakeholders. They should be translated into a corporate code of conduct, which could be used to control the behaviour of employees and establish moral codes for the organisation (Hinde, 2003).

The security of an organisation is only as strong as the weakest link, which is usually the employees, could put the organisation and its customers at risk. A code of ethics and conduct will facilitate responsible security awareness because users are personally responsible for ensuring sound security practices, which will lessen the security risks especially in an environment that is highly networked (Institute of Internal Auditors, 2001).
5. The oversight for the resource investment for information security

The reality facing most organisations is that even if the threat is understood with regard to information security, it is often hard to justify more than limited security measures because of the complexity involved and the investment in people, time and resources that is required. A very disturbing example on the issue of resource investment for information security is provided by Richard Clarke, the White House technology advisor, who states that most companies spend less on protecting their data as they do on coffee for their employees (Thomson, 2003a).

Price Waterhouse & Coopers further highlights this lack of financial support for information security in their alarming statistics from the 2002 Information Security Breaches Survey, as mentioned in section 5.2.3 (PriceWaterhouseCoopers, 2002). These statistics indicate the serious lack of resource investment in information security by the boards of companies. This lack of focus needs to be rectified.

6. The oversight for compliance with applicable legislation and regulations

The increase in information security intrusions and losses has escalated, as has the number of information security reports, laws and regulations. Carnegie Mellon University’s CERT Coordination Centre maintain that the quantity of cyber security incidents reported has approximately doubled each year since 2000, when 22000 incidents were reported, to 76000 in the first half of 2003 alone. This increase in incidents has been mirrored in the growth of reports, guidelines and new legislation (Business Software Alliance, 2003). Security breaches create a variety of litigation risks and the boards and senior executives of organisations can face legal liability in the event of these breaches. The need for sound risk processes within an organisation, an example of which is described in the King Report, means that focusing on developing, implementing and sustaining sound information security risk processes is critical. The board has a fiduciary responsibility for implementing sustainable risk management processes and meeting corporate governance requirements (Ernst and Young, 2005).
5.3. INFORMATION SECURITY AS A GOVERNANCE ISSUE

The board needs to be aware of all relevant legislation pertaining to information security. Standards for the compliance, review, monitoring and oversight functions must be incorporated into the overall security infrastructure to ensure that all legal requirements are met (Institute of Internal Auditors, 2001).

7. The oversight of investor relations and communications activity, including transparency

Effective information security governance can have a dramatic and positive impact on an organisation because it helps to build trusting relationships with its customers, suppliers and other business partners. This results in a strengthening of relationships with stakeholders, which is achieved by securing information through various security controls. This could ultimately improve the cash flow and profitability of the organisation (BS 7799, 1999).

Trust and confidence through oversight must be encouraged by the board. Governance, in general, deals with the core aspects of the business and how their content can be made transparent to the stakeholders of the corporation. Transparency deals with the degree to which shareholders receive a realistic representation of what is actually taking place within an organisation (Loyd, 2004). This applies equally to the governance of information security and its risks. Companies are increasingly making themselves more transparent to their customers, shareholders, employees and other stakeholders, especially in the area of risk. This has the advantage of encouraging the building of trust and confidence in the risk management of the company (Institute of Internal Auditors, 2000b).

These broad aspects form some of the pillars upon which information security governance should be built. It is wise for the board to take cognizance of all these elements and implement relevant policies ensuring their information asset is being protected and governed adequately and in a proper manner.
5.4 Reasons for Information Security Governance

The understanding of why information security should be governed is the first step to motivating the board and senior management to take ownership and become committed to information security. An organisation that implements security after a breach or incident has occurred can incur costs up to 100 times more than had they implemented the security precautions from the start (IT Governance Institute, 2001). Some of the reasons for implementing information security governance include (IT Governance Institute, 2001):

- The risks and threats to an organisation are real and can have a significant impact on the organisation;

- Coordinated and integrated action is required from the top down throughout the entire organisation to effectively implement information security;

- There are differing cultural and organisational factors which affect information security and are important in an organisation;

- Rules and priorities laid down by the board need to be established and enforced;

- Trust needs to be built up and demonstrated towards all trading partners especially with regard to the exchange of electronic transactions;

- Trust in the reliability in the security system needs to be demonstrated to all stakeholders;

- If security breaches do occur, reputational harm can be considerable, as security incidents will more than likely be exposed to the public.

Adequate and effective information security governance needs to be implemented by the board, but how should this be achieved?
5.5 Proposed Information Security Governance Program

It is essential, when implementing information security governance, that the framework being implemented is built on existing frameworks and accepted best practices. Entrust (2004) maintains that information security programs often fail to involve the board and executive management in the risk assessment and remediation process. Any weaknesses in information security create real business risk and the responsibility for information security ultimately lies with the CIO (as per the proposed structure in Chapter Three), the CEO and the board of directors. Only the board and senior executives can determine an acceptable risk profile, focus information security investments appropriately and drive the results.

It is important to keep the ISG process as simple as possible. This can be done by maintaining focus on improving the security posture of the organisation rather than performing complex risk analyses. The program should begin with identifying the most important items that will have the greatest impact, and where the business need is the most. It is important to remember that changes in technology and environmental threats can emerge overnight resulting in new vulnerabilities that need to be addressed. Therefore, the task is never finished and must continually be re-assessed and remedied.

A framework needs to be implemented, which includes questions (these will be addressed in Chapter Six) that should be asked by the board and senior management to successfully implement information security governance. These questions require answers to ensure an adequate level of information security governance is being applied. Performance measurements and monitoring, with reporting, are other important facets of implementing information security governance.

A proposed matrix, with supporting modular activity plans, is developed in Chapter Seven with guidelines for implementing both information security governance and information technology governance. Its purpose is to facilitate the board and senior management in the implementation of the critical function of corporate information governance.
5.6 Conclusion

Information security governance strives to secure the information asset at an executive level and it will ultimately enable the organisation to maintain a competitive edge, cash flow, profitability, legal compliance and lastly, the company reputation. The provision of good information security governance is expensive, but information security is a fundamental and unavoidable cost of doing business and when provided in a timely and effective manner can protect the health of the company and enable competitive advantage and new business opportunities (Institute of Internal Auditors, 2000b). Thus, information security governance needs to be seen by the board as an opportunity and not a challenge. Weak information security governance creates a real business risk and the responsibility for information security lies with the CIO (as proposed in Chapter Three), the CEO and the board of directors. It is the responsibility of the board to determine an acceptable risk profile, focus the information security investments appropriately and drive the results (Entrust, 2004a).

Chapter Three has introduced the concept of corporate information governance, with the suggestion that the CIO has a seat on the board and is charged with the specific responsibility of the information asset. It further proposed that corporate information governance be divided into two main components and that a separate study of each component was warranted.

Chapter Four appears to have justified the scrutiny of the governance of information technology at the highest level.

Chapter Five has confined itself to a study of the second component of corporate information governance, namely the governance of information security. This explored issues of information security and its governance elements, such as confidentiality, integrity, availability, risk, compliance and ethics amongst others. It draws the conclusion that information security governance is equally as important as information technology governance and that both form the basic pillars constituting corporate information governance.

Chapter Six will bring these two components together by extracting the fundamental issues of each, from their relevant chapters. These fundamental issues are presented in the format of questions the board should be asking
to ensure an adequate corporate information governance process. This will highlight the importance with which the board views both these components as important governance issues.
Part III

Solution
Chapter 6

Core Aspects and Fundamental Issues

Chapter 6:
6.1 Introduction
6.2 Core Aspects and Fundamental Issues
6.3 Questions and Answers
6.4 Conclusion
6.1 Introduction

Chapters Four and Five have discussed the two components of corporate information governance in depth. It became increasingly apparent, from early in the literature study, that certain "fundamental issues" were appearing with regularity. These fundamental issues appeared in the literature study of both the governance of information technology and the governance of information security.

This chapter illustrates that these fundamental issues can be placed into four specific groups or core aspects, as they are called. These core aspects are discussed briefly in this chapter to identify what they entail. They form part of the matrix and supporting modular activity plans that are developed in Chapter Seven and are discussed in greater detail in this chapter.

This chapter groups the fundamental issues, gleaned from Chapters Four and Five, with their associated core aspect. These fundamental issues are presented in the format of questions the board should be asking to ensure an adequate corporate information governance process. This will highlight the importance with which the board views both these components as important governance issues.

At the conclusion of this chapter, a tabular summary of the core aspects and the questions, is presented illustrating the fundamental issues and demonstrating their significance to IT governance and IS governance.

6.2 Core Aspects and Fundamental Issues

Some fundamental issues were highlighted in Chapters Four and Five relating to the governance of information technology and the governance of information security. Fourteen fundamental issues were extracted because they represent the most important issues highlighted in each of the chapters to combine the research done on each component of corporate information governance. The following fundamental issues illustrate that the effective governance of the information asset is, with respect to IT and IS:

- critical to the organisation;
- a direct board responsibility;
6.2. CORE ASPECTS AND FUNDAMENTAL ISSUES

- needs more attention from the board;
- has strategic issues involved;
- requires large investments from the organisation;
- able to enhance competitive edge;
- requires transparency;
- enhanced by compliance;
- enhanced by following codes of best practice;
- enabled when investments are made that are commensurate with the risks involved;
- enabled when education, awareness and training is implemented in the organisation;
- enabled when performance is measured and monitored;
- enabled when implemented on a continuous basis;
- enabled when roles and responsibilities are assigned to ensure accountability.

The fundamental issues will be turned into questions the board should ask to determine their relevance and validity with respect to information technology and information security governance.

The closer examination of these issues revealed that all these fundamental issues can be placed into four groups or core aspects, as they are called for the purposes of this dissertation. (It is not claimed that these four groups are a comprehensive/complete list.) These core aspects from the “Board briefing on IT Governance” by the IT Governance Institute (2004) (IT Governance Ltd, 2004a) include:

- Core Aspect 1: Strategic Planning;
- Core Aspect 2: Value Delivery;
- Core Aspect 3: Risk Management;
Core Aspect 4: Resource Management.

The reason for choosing these core aspects as groupings for these fundamental issues is because the IT Governance Institute is renowned as an authoritative body on information technology and information security governance and is well accepted as an authority in IT governance circles. The core aspects form part of an IT governance framework suggested by the IT Governance Institute and have been adapted for the purpose of this dissertation. These four core aspects form part of the proposed Corporate Responsibility Matrix and Modular activity plans and are discussed in greater detail in Chapter Seven, but for the purpose of this chapter are used as groupings for the fundamental issues.

The following format will be used to illustrate how the groupings of the fundamental issues or questions will be achieved:

Core Aspect 1: Strategic Planning
Fundamental Issue 1.1 Question
With reference to the Governance of Information Technology - Answer
With reference to the Governance of Information Security - Answer
Fundamental Issue 1.2 Question
With reference to the Governance of Information Technology - Answer
With reference to the Governance of Information Security - Answer

First, the core aspect is stated. Next, the fundamental issues, in the form of a question are asked. The answers are taken from Chapter Four, with regard to firstly, the governance of information technology, and then secondly, from Chapter Five, with regards to the governance of information security. These answers validate the importance of both components of corporate information governance as vital governance issues.

A brief summary of each core aspect and its relevance to each of the fundamental issues will further explain the reason for grouping specific fundamental issues under specific core aspects.

Core Aspect 1: Strategic Planning pertains to the development of a corporate information strategy that generates the objectives and goals of the organisation in specific areas relating to IT and IS. Thus, the fundamental
issues that relates to the concept that the proper governance of the information asset is critical to an organisation, will be grouped under the core aspect of strategic planning because it is of strategic importance. The second, third, fourth and fifth fundamental issues or questions, of whether the governance of the information asset should be a direct board responsibility, whether the board should give more attention to the governance of the information asset, whether the governance of the information asset has strategic issues involved and lastly, whether it requires or should require large investments from the organisation, are all of strategic importance and therefore, are grouped under the Core Aspect 1.

Core Aspect 2: Value Delivery pertains to optimising expenses and proving the value delivered from both IT and IS. Thus, the fundamental issues or questions on competitive advantage and transparency both pertain to adding value to the organisation and therefore, have been grouped with this Core Aspect.

Core Aspect 3: Risk Management pertains to the safeguarding of the information asset and business continuity. The fundamental issues of compliance and the following of codes of best practice all relate to risk management and will be grouped under this core aspect.

Core Aspect 4: Resource Management pertains to the optimal management and allocation of resources including the human resource. The fundamental issue or question on ensuring the investments into IT and IS are commensurate with the risks involved, could have been placed with the previous core aspect. It was decided however, that because it has to do with the investment into resources, it would be placed under this core aspect. The last four fundamental issues of education, awareness and training; performance measurement; continuous implementation; and roles and responsibilities all pertain to resource management and allocation and therefore, have been grouped under this heading.
6.3 Questions and Answers

6.3.1 Core Aspect 1: Strategic Planning

This pertains to the development of a corporate information strategy, that generates the objectives and goals of the organisation in specific areas relating to IT and IS.

Fundamental Issue 1.1: Is the proper governance of the information asset critical to an organisation?

With reference to the Governance of Information Technology

Richard Nolan, a Harvard Business School Professor, was asked in an interview by CIO Insight as to why it was so critical that boards pay closer attention to information technology and he replied that 55% of the capital investment of an average company is “funneled into” information technology and this high level of investment demands more senior management attention. He continued that another important reason for board involvement was that the role of information technology is expanding so rapidly both into and across organisations that the decisions that are made, affect entire networks of companies (Alter, 2004). Every organisation today is dependent upon information technology and interconnected in some way or another and therefore, the effective governance of information technology is critical to an organisation and its stakeholders.

With reference to the Governance of Information Security

It is a known fact that organisations are increasingly dependent on information systems. The IT Governance Institute (2001) maintains that as this dependency on information systems continues to grow, so too does the criticality of information security, bringing with it the need for effective information security governance.

Fundamental Issue 1.2: Should the board be responsible for the proper governance of the information asset?

With reference to the Governance of Information Technology

The board is ultimately responsible for the protection and governance of
the information asset. The IT Governance Institute (2003) states that information technology governance is the responsibility of the board of directors and senior executives and needs to be an integral part of its overall corporate governance structure. It should not be seen as an isolated discipline, separate from the rest of the organisation, but rather needs to be elevated to board level ensuring that it is governed adequately.

**With reference to the Governance of Information Security**

The boards of organisations have, on the whole, considered information security to be a technical issue only and not as a governance issue. They will, increasingly, be expected to make information security an intrinsic part of governance and therefore, should integrate information security governance into the process they have in place to govern information technology because both need to be overseen by the board to be effectively governed (IT Governance Institute, 2001).

**Fundamental Issue 1.3: Does the proper governance of the information asset require more board-level attention?**

**With reference to the Governance of Information Technology**

The focus of the board is mainly on business strategy and strategic risks and few boards focus directly on information technology, despite the fact that it involves large investments and huge risks (IT Governance Institute, 2003). This is, generally, because information technology has been treated as a separate entity to business because of its complexity. This needs to be rectified and therefore, for the governance of information technology to be adequate and effective, more board-level attention is required.

**With reference to the Governance of Information Security**

The previous statements apply equally to information security. It is, usually, treated as a technology issue when it should be treated as a governance issue. Therefore, little attention is often given to this issue at board level, resulting in information security efforts being frequently under-funded in proportion to the risk and magnitude of the harm that incidents could produce (Business Software Alliance, 2003). Information security is often seen as a negative factor, creating value through nonoccurrence. The main cause for
this lack of attention by the board is that security is treated as an overhead rather than an investment (PriceWaterhouseCoopers, 2002). Greater involvement of the board is required for information security to be properly addressed. The board should consider information security in the light of its ability to create value and build opportunity (IT Governance Institute, 2001).

**Fundamental Issue 1.4: Are there strategic issues involved in the proper governance of the information asset?**

**With reference to the Governance of Information Technology**

Senior management and the board are realising increasingly that the strategic value of information technology and the significance it can have on the success or failure of their organisation. Therefore, they are now striving to successfully leverage information technology opportunities for their competitive advantage. It is important for the board to know whether their information technology strategic plans are likely to achieve their objectives and be resilient enough to adapt to changes and growth. The board equally needs to know if the risks are being managed judiciously and lastly, whether appropriate opportunities presented by the information technology are being recognised and capitalised on (Trites, 2004). Thus, the governance of information technology involves many strategic issues.

**With reference to the Governance of Information Security**

There are definitely strategic issues involved with information security governance. One of the strategic issues include ensuring that security requirements are driven by the organisational requirements, by providing a strategic alignment of information security governance with the business strategies. Security solutions need to fit in with the organisational processes already in place and the investments in information security need to be aligned with the business strategy and the agreed-upon risk profile (IT Governance Institute, 2001).

A reason for concern about information security at board level, is the enabling of the business strategy, as increasingly, information security is becoming a vital aspect of creating and sustaining trust between organisations and their business partners, customers and employees (Ernst and Young, 2005).
This means that a strong alignment between business, technology and the information security strategies is required. Therefore, there are many strategic issues to be considered concerning the governance of the information security of an organisation.

**Fundamental Issue 1.5: Does the proper governance of the information asset require the organisation to outlay large investments?**

**With reference to the Governance of Information Technology**

The statistics revealed that 55% of the capital investment of an average company was being invested into information technology (Alter, 2004) in 2003. This constitutes a large amount of money being outlayed by the organisation into information technology and this, in turn, necessitates the attention of the board.

**With reference to the Governance of Information Security**

The investments into information security have not been adequate up till now. Little attention is given to information security at board level and the result is that information security efforts are frequently under-funded when weighed against the risk and magnitude of the harm that security breaches could produce (Business Software Alliance, 2003). A disturbing example, about the issue of investment into information security, was described in Chapter Five, that most companies spend less on protecting their data than they do on coffee for their employees. It is estimated that less than 0.0025% of corporate revenue is spent on corporate information security protection (Thomson, 2003a). This needs to be rectified. The provision of good information security governance requires a larger investment of money, and is a fundamental, unavoidable cost of doing business in the world currently (Institute of Internal Auditors, 2000b).
6.3.2 Core Aspect 2: Value Delivery

This pertains to optimising expenses and proving the value delivered from both IT and IS.

**Fundamental Issue 2.1: Is maintenance of competitive edge a governance issue?**

**With reference to the Governance of Information Technology**

Information technology governance needs to ensure that IT investment decisions are not just aligned with the business strategic objectives, but that they are derived from an IT strategy, which itself is derived from an appropriate analysis of organisational business objectives. This leads to investment decisions that *enhance competitive advantage*, improve business processes and contribute to growth that both protects and enhances shareholder value (IT Governance Ltd, 2004b). It is important that the board to take cognizance of the opportunities to *enable and sustain competitive advantage* with the adequate governance of information technology.

**With reference to the Governance of Information Security**

Information security governance strives to secure its information asset at an executive level and it ultimately enables the organisation to *maintain competitive edge*, cash flow, profitability, legal compliance and lastly, its reputation. The provision of good information security governance in a timely and effective manner can protect the health of the company, *enable a competitive advantage* and new business opportunities (Institute of Internal Auditors, 2000b).

**Fundamental Issue 2.2: Is transparency an important issue for the proper governance of the information asset?**

**With reference to the Governance of Information Technology**

A climate of trust and confidence can be achieved through *transparency*. A greater need is arising for corporate transparency and accountability, where companies for the first time make themselves clearly visible to shareholders and other stakeholders in all aspects of governance, but especially with regards to their risks. *More transparency* engenders more confidence and...
likewise, a lack of transparency can result in a lack of trust, which could be detrimental to the organisation (Institute of Internal Auditors, 2000b).

**With reference to the Governance of Information Security**

Companies need to provide access to their information and services with the increased need for growth and sustained competitive advantage. There is a constant balancing act being performed within organisations to be open, transparent and accessible, while still complying with the myriad of governmental regulations concerning information security. This balancing act depends on secure information systems. Transparency and accessibility produce their own inherent risks, but these need to be leveraged to enable the organisation to take advantage of their opportunities (Entrust, 2004b).

### 6.3.3 Core Aspect 3: Risk Management

This pertains to the safeguarding of the information asset and business continuity.

**Fundamental Issue 3.1: Is compliance an issue in the proper governance of the information asset?**

**With reference to the Governance of Information Technology**

A function of information technology governance includes ensuring compliance with legislation, standards, regulations, best practices etc., that pertain to IT. Information technology governance needs to create a climate of trust and confidence through oversight (Loyd, 2004). Therefore, the oversight and governance of information technology must address compliance as an issue to adequately govern the information asset.

**With reference to the Governance of Information Security**

*Compliance is an important issue*, as far as the governance of information security is concerned. Senior executives and the board need to ensure the well-being of the organisation as part of good corporate governance practices. The board provides direction and guidance to the organisation to achieve its goals and objectives. This is generally accomplished through the creation and implementation of management policies and programs. One such policy
is the Corporate Information Security Policy, which is used to direct the use and protection of the organisation’s information asset. (Krause & Tipton, 1998). There are circumstances where a court of law may find that a company without an information security policy or practice in place, has failed to take the necessary steps to provide adequate confidentiality and security of the data of their customers (Gordon and Glickson LLC., 1998). Compliance by employees to the Corporate Information Security Policy is a must and needs to be constantly monitored by management. The board, on the other hand, needs to ensure compliance to goals and objectives by management.

There have been several regulatory and legal developments with regard to information security over the past few years. The board needs to ensure that their organisation comply with those that are applicable to their industry. Some examples of laws and regulations applicable to information security include the European Community Directive on Privacy, Healthcare Industry Privacy and Accountability Act (HIPPA), Sarbanes-Oxley Act, Electronic Communications and Transactions Act (ECT Act) of South Africa and the Companies Act. It is important that senior executives and the board ensure that their Corporate Information Security Policy and practices are in line with local and international guidelines, codes of practice and legal requirements because this can help reduce the liability of the organisation.

Good information security governance, according to Swindle and Connor (2004), provides more than just legal or compliance benefits, but could serve as a “catalyst to even greater productivity gains and cost efficiencies for businesses, customers, citizens and governments during times of crisis and normal operations.”

Fundamental Issue 3.2: Should best practices be followed for the proper governance of the information asset?

With reference to the Governance of Information Technology

It is beneficial for an organisation to seek out and study the practices used in other organisations to possibly improve their own. An example of an established IT governance code of best practice is the Control Objectives for Information and Related Technology (CobiT). It was created to align IT resources and processes with business objectives, quality standards, monetary controls and security needs. The company, Dell Computers, has a reputation
of having high quality standards. They have stated that the incorporation of CobiT best practice, as part of its Control Self Assessment (CSA) corporate policy, has helped the company to maintain this high standard of quality (Oltsik, 2003).

**With reference to the Governance of Information Security**

Prof B. von Solms (2001) maintains that a code of best practice can provide the organisation with a reference framework ensuring that information security aspects are covered. These documents can be used to ensure that they are addressing most of their information security risks, without necessarily executing a comprehensive risk analysis exercise (von Solms, 2001b). A board wishing to govern their information security adequately should seriously consider ensuring that some applicable code of best practice is being implemented within their organisation.

### 6.3.4 Core Aspect 4: Resource Management

This pertains to the optimal management and allocation of resources including the human resource.

**Fundamental Issue 4.1: Is it important for investments to be commensurate with risks for the proper governance of the information asset?**

**With reference to the Governance of Information Technology**

Information technology becomes more critical to organisations and more pervasive and companies are increasingly being challenged to manage and govern their information technology assets more effectively and efficiently ensuring they balance the opportunities of the new technology with the risks that they inherently carry. Chapter Four highlighted that the board needs to be aware of emerging technologies, operations, architecture and strategic potential. The board needs to know that their IT infrastructure is sound and unlikely to collapse due to obsolescence and cost millions to rectify. This is the kind of surprise that the board does not need and ought not to happen (Alter, 2004). Thus, the allocation and management of resources is an important function that needs to be addressed by the board. It needs to ensure
adequate resources are being invested into information technology to remain competitive and productive and they need to be aware of the inherent risks that new technology can introduce into the organisation.

**With reference to the Governance of Information Security**

The decision, as to the *amount of appropriate resources to be invested in information security*, is made through recommendations by management and the concurrence of the board. The Y2K problem showed many CEOs and corporate directors how dependent their organisations were on information technology and how operational risk can create a serious business risk (Institute of Internal Auditors, 2001). The denial of service attacks, in February 2000, on Amazon.com, eBay and other web sites, had serious negative repercussions on the valuation of their stock. How much security is enough is a critical and yet difficult question to answer. Donn B. Parker, Consultant Emeritus, SRI International says that security in a cyber-world is no longer an issue of how much risk can be tolerated because the risk has already materialized, occurring with increasing frequency and causing massive losses. Security is necessary merely to enable electronic commerce to function. One does not need to know the risk of failing to decide to install security any more than one would need to know the risk, before putting a lock on one’s front door. It’s basically common sense, good practice and due diligence (Institute of Internal Auditors, 2001). It is *vital for the board to acknowledge that investments in information security must be commensurate with the risks* that face an organisation on a daily basis.

**Fundamental Issue 4.2: Are education, awareness and training necessary for the proper governance of the information asset?**

**With reference to the Governance of Information Technology**

One of the objectives of an effective information technology governance process is to *encourage desirable organisational behaviours*, but too often, business and information technology governance just ””happen”. The definition of desirable behaviours takes time, effort and focus. It is important for the board to realise that an effective information technology governance process is not a “one size fits all”. It differs from organisation to organisation due to the desired business objectives and the behaviour sought (Weill
& Broadbent, 2003). Thus, ongoing education, awareness and training, with regard to information technology, is imperative for any organisation and it is the responsibility of the board to ensure that the correct skills are available to take advantage of opportunities as they arise to remain competitive within their industry.

**With reference to the Governance of Information Security**

Security awareness and education are vital to an organisation wishing to ensure that all its stakeholders embrace the culture of security (Pounder, 2002). The education of its employees, on an ongoing basis, is essential to ensure that security awareness is always uppermost in the minds of the employees. This promotes the responsible use of computers within the organisation and will minimise the risk of unauthorised access and irresponsible behaviour. It is believed that as much as 80% of security problems stem from a lack of understanding or carelessness and not from any direct attack. Some examples of security problems include shoddy administration, sharing of passwords and needlessly leaving computers logged on and unattended, which could lead to security breaches. All of these examples of lack of security could be prevented through education, training and awareness (Institute of Internal Auditors, 2001).

**Fundamental Issue 4.3: Is performance measurement necessary for the proper governance of the information asset?**

**With reference to the Governance of Information Technology**

The main purpose of information technology governance is to direct and control information technology projects, ensuring that the performance of information technology meets the strategies and goals set by the board. The performance is measured to ensure compliance. The use of information technology needs to enable the enterprise by exploiting the opportunities and maximising the benefits through the responsible use of the resources and needs to be monitored and measured (IT Governance Institute, 2003). Therefore, performance measurement is essential to ensure that compliance to strategies, goals and objectives is being achieved at all levels of the organisation.
With reference to the Governance of Information Security

Information security risk management will be successful when the roles and responsibilities are assigned to ensure that there can be accountability. There will exist various information security structures within an organisation and performance measurement, monitoring and deviation analysis must occur to identify security breaches. This analysis must contain an executive level planning to counteract these deviations. This enables the board to actively protect the information asset of the enterprise. This is an ongoing exercise that requires the highest level of commitment from the board to minimise both technical and non-technical risk (IT Governance Ltd, 2004b).

Fundamental Issue 4.4: Should continuous evaluation take place for the proper governance of the information asset?

With reference to the Governance of Information Technology

The process of information technology governance starts with the setting of clear objectives and principles for the information technology of the organisation, defining the role that it will play within and across the organisation and thus, providing the initial direction. Next, the roles and responsibilities of the different levels of the organisation need to be assigned to enable accountability (Gerrard, 2004). Subsequently, a continuous cycle is established for measuring performance, comparing objectives, resulting in the redirection of activities where necessary and including a change of objectives where appropriate. The setting of objectives and principles is primarily the responsibility of the board and requires senior executive buy-in and sponsorship. This will, in turn, provide the oversight and strategic direction and support for the process. The measuring of performance is the responsibility of management and it is important that the setting of objectives and principles and the measuring of performance is developed in tandem ensuring that the objectives are achievable and the measures represent the objectives correctly (IT Governance Institute, 2003).

With reference to the Governance of Information Security

The board, or another appropriate committee, should ensure that the required periodic information security reporting by management is being performed and that, ideally, independent assessments are done by internal and
6.3. QUESTIONS AND ANSWERS

external auditors. This must be a continuous process and like due diligence, the assessing of information security is continuous. It is important to remember that an assessment tool, such as, internal controls must be flexible and reviewed regularly. John Lindquist, President and CEO, EWA Information and Infrastructure Technologies, Inc., stated that an organisation needs to protect its information assets, not its computer systems. The problem is a risk management problem dealing with people, process and technology. All three must be integrated to protect the information asset and must be continuous. He suggested that each part of the solution has about an 18-month half-life and that it must never be considered a “fix and forget” solution (IT Governance Ltd, 2004b).

Fundamental Issue 4.5: Should roles and responsibilities be assigned for the proper governance of the information asset?

With reference to the Governance of Information Technology

Peter Weill, Senior Research Scientist and Director CISR, MIT Sloan School (2002) states that information technology governance is defined as specifying the decision rights and introducing an accountability framework to encourage desirable behaviour in the use of information technology. The board needs to assign the roles and responsibilities of the different levels of the organisation ensuring accountability after setting objectives and goals for the organisation (Gerrard, 2004). Good practices in information technology governance need to be applied throughout the organisation and especially, between the information technology function and the business units. Each level within an enterprise needs to have specific roles and responsibilities assigned, for example, the board needs to take an active role in information technology strategy; the CEO should provide organisational structures to support the implementation of information technology strategy; the CIO must be business-oriented and provide a bridge between the information technology and the business; business units need to work in partnership with information technology to ensure that their business requirements are met (IT Governance Institute, 2003). It is evident that the assigning of roles is important because individuals are aware of their responsibilities and can be held accountable when things go awry.
With reference to the Governance of Information Security

Information security risk management will be successful when roles and responsibilities are assigned to ensure accountability. Management is responsible for providing information security, while the board is accountable, as part of its duty of care, to provide effective information security oversight (Institute of Internal Auditors, 2001) It is important that roles and responsibilities are assigned to individuals so that responsibility and accountability can be measured and monitored.

Table 6.1 is a tabular representation of the four Core Aspects and their related fundamental issues. It indicates the relevance of the questions or the fundamental issues in relation to the governance of information technology and the governance of information security. It can be seen from the summary that both components - the governance of information technology and the governance of information security, have relevance with regard to all the core aspects and fundamental issues.

### 6.4 Conclusion

It was stated in the introduction that the literature studies in Chapters Three, Four and Five have revealed that the governance of the information asset revolves around several fundamental issues. The literature has stated further that there are four key groups of the governance of information technology and the governance of information security and these have been named “core aspects”, for the purposes of this dissertation, thus enabling the allocation of these fundamental issues to the relevant core aspect (IT Governance Ltd, 2004a).

It is particularly important to reveal that with all of the fundamental issues, the governance of information security has shown itself to be at least as important as the governance of information technology. The literature study has revealed that the overwhelming application of corporate resources has been assigned to the governance of information technology and not shared equally with information security. It now appears probable that this phenomenon could be one of the reasons for the corporate failures or losses mentioned in Chapter Two. The overall benefits accruing to an organisation
### Table 6.1: Tabular Summary of Core Aspects and Fundamental Issues

<table>
<thead>
<tr>
<th>Fundamental Issue No</th>
<th>Questions</th>
<th>IT</th>
<th>IS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Core Aspect 1: Strategic Planning</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.1</td>
<td>Is the proper governance of the information asset <strong>critical</strong> to the organization?</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>1.2</td>
<td>Should the <strong>board</strong> be responsible for the proper governance of the information asset?</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>1.3</td>
<td>Does the proper governance of the information asset require <strong>more board-level attention</strong>?</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>1.4</td>
<td>Are there <strong>strategic issues</strong> involved in the proper governance of the information asset?</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>1.5</td>
<td>Does the proper governance of the information asset require the organization to outlay large investments?</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td><strong>Core Aspect 2: Value Delivery</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.1</td>
<td>Is the maintenance of <strong>competitive edge</strong> a governance issue?</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>2.2</td>
<td>Is <strong>transparency</strong> an important issue for the proper governance of the information asset?</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td><strong>Core Aspect 3: Risk Management</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.1</td>
<td>Is <strong>compliance</strong> an issue in the proper governance of the information asset?</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>3.2</td>
<td>Should <strong>best practices</strong> be followed for the proper governance of the information asset?</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td><strong>Core Aspect 4: Resource Management</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.1</td>
<td>Is it important for <strong>investments</strong> to be commensurate with risks for the proper governance of the information asset?</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>4.2</td>
<td>Are <strong>education, awareness and training</strong> necessary for the proper governance of the information asset?</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>4.3</td>
<td>Is <strong>performance measurement</strong> necessary for the proper governance of the information asset?</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>4.4</td>
<td>Should <strong>continuous evaluation</strong> take place for the proper governance of the information asset?</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>4.5</td>
<td>Should <strong>roles and responsibilities</strong> be assigned for the proper governance of the information asset?</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
from the proper governance of the information asset are considered and another probable cause of corporate failures or crises could also be a matter of lack of expertise at senior management and board level.

This chapter has attempted to successfully address one of the secondary objectives stated in Chapter One by motivating the importance of both information technology and information security as governance issues.

The primary objective of this dissertation has been to evaluate the governance of the information asset as it has been applied to assess the viability or otherwise, of current practice and to propose solutions for resolving identified problem areas. The studies have yielded findings of value and it appears appropriate to propose a structure for improving the implementation of the governance of the information asset, based on these findings. This structure, called the Corporate Responsibility Matrix, is discussed in the following chapter and as a detailed discussion of the four core aspects and how they are used in the development of the matrix. Four modular activity plans are presented and discussed in detail in the next chapter to practically facilitate the board in implementing an improved corporate information governance process.
Chapter 7

A Corporate Responsibility Matrix

Chapter 7:
7.1 Introduction
7.2 Criteria for the development of a Corporate Responsibility Matrix
7.3 Process of Corporate Information Governance
7.4 Components of the matrix
7.5 The Corporate Responsibility Matrix
7.6 Benefits of implementing the matrix
7.7 Conclusion
7.1 Introduction

There were two identified components of corporate information governance proposed in Chapter Three, namely the governance of information technology and the governance of information security. Chapter Six highlighted the important issues concerning these two components by introducing core aspects and fundamental issues. The important fundamental issues resulted in questions to which answers were given that had been extracted from Chapters Four and Five, illustrating the similarity between these two components with respect to their importance as governance issues. Each fundamental issue was placed under its respective core aspect, as these will be used in the development of a three-dimensional matrix and Modular Activity Plans in this chapter. The purpose was to illustrate how these core aspects with their associated fundamental issues could be used by the board to improve their corporate information governance process.

This chapter proposes a format of activities, named here as a Corporate Responsibility Matrix which has, as its objective, the promotion of an optimized process for the governance of the information asset. This chapter begins with the criteria deemed necessary for the development of the Corporate Responsibility Matrix. These criteria are followed by an illustration and discussion on the process of corporate information governance and a description of the different components of the Corporate Responsibility Matrix, namely the Directing, Controlling and Responsibility components and the reasons for choosing these components.

The next section illustrates and discusses the Corporate Responsibility Matrix. Its purpose is to bring together the important functions of corporate governance, articulate the core aspects, assign ownership of them, and evaluate performance and compliance. A discussion around this matrix will address the core aspects (as presented in Chapter Six), namely Strategic Planning, Value Delivery, Risk and Resource Management, which make up the Directing dimension and a discussion of roles and responsibilities and those general principles of control management applicable to this structure.

Suggested Modular Activity Plans are proposed as a support for the Corporate Responsibility Matrix. Their purpose is the practical implementation of an improved corporate information governance process. These Modular
7.2. CRITERIA FOR THE DEVELOPMENT OF A CORPORATE RESPONSIBILITY MATRIX

Activity Plans are discussed around each core aspect. A short discussion on the layout of the Modular Activity Plan explains their structure.

The Corporate Responsibility Matrix and Modular Activity Plans are important because incorporated together, they provide a means for the implementation, evaluation and improvement of the corporate information governance process. They enable the board to ensure that all aspects of corporate information governance are implemented adequately.

Lastly, this chapter closes with the benefits of implementing this Corporate Responsibility Matrix and the Modular Activity Plans as proposed. A brief discussion on the criteria required for the development of the proposed Corporate Responsibility Matrix is presented in the next section.

7.2 Criteria for the Development of a Corporate Responsibility Matrix

The following activities should be considered when developing criteria for designing a conceptual responsibility matrix, whether it be for IT governance, IS governance, or corporate information governance (IT Governance Institute, 2001):

- Policy Development and Direction Setting - ensure that strategies, core principles and objectives are set by the board and senior management;

- Roles and Responsibilities - individual roles, responsibilities and authority levels need to be clearly communicated and understood by all;

- Control Measures - ensure that control measures are established to detect and ensure correction of non-compliance to objectives and goals set by the board;

- Awareness, Training, Education and Motivation - ensure that awareness of the need to protect corporate information has a high priority throughout the organisation, promote skills training and education in security measures and practices. Motivation is crucial because even though people are aware of how to act, they often need to be motivated to comply.
Once the organisation has developed the criteria required for the corporate information matrix, it would be wise to examine the proposed process of corporate information governance. This process gives a broad outline of the responsibilities and activities of the board, CEO’s and CIO in respect to the governance of the information asset.

7.3 Process of Corporate Information Governance

The process of corporate information governance is illustrated in Figure 7.1. This figure is developed from the following information. The board needs to ensure the strategic direction of the company by setting strategies and objectives with regard to IT and IS (Organisation for Economic Co-operation and Development, 2004). These strategies and objectives have been extracted from important aspects highlighted in Chapters Four and Five. The strategies and objectives of the board should include the need to ensure that IT and IS strategies are aligned with the business strategies; to ensure that IT and IS enable the business and deliver value; to ensure all the resources available for IT and IS are allocated and managed responsibly; to ensure all the IT and IS related risks are defined and managed. These strategies and objectives mirror the core aspects as presented in Chapter Six, and form part of the Directing function of the board. These core aspects are discussed in more detail in the next section.

The CEO, according to the King Report (2001), needs to consistently drive the company to achieve the strategies and objectives of the board. This is achieved with the help of the CIO, who needs to take the responsibility of achieving the strategies and objectives of the board, with regard to IT and IS (Entrust, 2004a). These activities include increasing efficiency, profitability and security of the organisation.

The Controlling function comes into play in the measuring and monitoring of performance within the organisation. Furthermore, redirection or remedial action may need to occur to achieve the strategies and objectives of the board (Entrust, 2004a).

The proposed components that make up the Corporate Responsibility
Matrix for the governance of the information asset, will be briefly discussed, indicating why the relevant components were chosen.

### 7.4 Components of the Matrix

Corporate information governance was defined in Chapter Three, as the systematic oversight and execution of information security and information technology functions and operations. Corporate information governance, as a subset of corporate governance, needs to incorporate the main functions of corporate governance, those of Directing and Controlling, while assigning roles and responsibilities to the different levels of the organisation to ensure accountability (King Report, 2001). The board and senior management can no longer merely issue directives, educate users and then expect compliance (IT Governance Institute, 2001). The speed with which risks emerge and technology changes requires a different and continuous approach. It implies continuous monitoring and testing of the infrastructure and environment for vulnerabilities and the required response, in terms of remedial measures, is executed through the IT and IS management function, improved defenses and changed policies.

Corporate information governance, like most other governance activities,
engages both the board and executive management in a cooperative manner. The board, the CEO and the CIO (as proposed in Chapter Three) must set direction and insist on control, while relying on the lower levels of the organisation to provide the information required for decision-making and evaluation activities due to the complexity and specialisation of this governance activity (Business Software Alliance, 2003). This is achieved by assigning roles and responsibilities, measuring performance and compliance, and redirecting when necessary.

The basic functions of corporate governance - Directing and Controlling - are used to form the first two dimensions of the three-dimensional Corporate Responsibility Matrix (King Report, 2001). The Responsibility component forms the third dimension of the matrix to ensure accountability (Institute of Internal Auditors, 2000b). The specification of who does what, allows an organisation to assign specific tasks and responsibilities and a means of measuring or monitoring to ensure compliance. Therefore, the following three components are included in the Corporate Responsibility Matrix, namely:

- A. Directing Components - what is required;
- B. Controlling Components - is there compliance?
- C. Responsibility Components - who must do it.

These three components of the three-dimensional Corporate Responsibility Matrix are discussed in more detail after illustrating the matrix.

### 7.5 The Corporate Responsibility Matrix

The Corporate Responsibility Matrix, as illustrated in Figure 7.2, was designed to show firstly, the two major functions of the board, which include the Directing and Controlling functions (King Report, 2001). The third component that was deemed important, was the allocation of responsibilities to different levels of management to allocate tasks and activities (Institute of Internal Auditors, 2000b).

The purpose of the Corporate Responsibility Matrix is to combine the important aspects of corporate information governance and use this as a basis for the design of the Modular Activity Plans. These Modular Activity
Plans, in turn, demonstrate the interconnection between the three dimensions of the Corporate Responsibility Matrix and can be used facilitate the board in practically implementing an improved corporate information governance process.

The Directing component (A.) are divided into the four core aspects of corporate information governance as introduced in Chapter Six, namely Strategic Planning (A1), Value Delivery (A2), Risk Management (A3) and lastly, Resource Management (A4) (IT Governance Ltd, 2004a).

The board has a responsibility to retain full and effective control over the organisation and the monitoring of management in the implementation of board plans, goals and strategies (King Report, 2001). The Controlling component (B.) of the matrix will consist of Performance Measurement (B1), Deviation Analysis (B2) and Reporting (B3). The Controlling functions do not begin and end at board level and need to be implemented at all levels of the organisation ensuring that compliance with the strategies and objectives of the board can be measured and monitored. These strategies and objectives are communicated to senior management, who in turn, trans-
late them into action plans for execution by the staff. Many of these action plans are designed around a budget versus target versus actual format. This is done to simplify the control mechanisms of measurement and evaluation through periodic report backs from lower levels of management to senior management. Senior management, in turn, are obliged to report progress back to the board and produce remedial or redirection plans for board approval when deviations from targets have occurred. These redirecting plans are made possible via, for example, the mechanism of potential deviation analysis, which poses the questions ‘If this, then what?’ The board needs to satisfy itself that this entire process is in place and that deviation correction plans exist.

The Responsibility component (C.) indicates the four suggested levels of management, namely board of directors (BoD) (C1), CEO (C2), CIO (C3) and Unit Heads (C4). A set of activities or tasks will be proposed and allocated to each level of Responsibility for each core aspect.

7.5.1 Modular Activity Plans

The purpose of the Modular Activity Plan is to illustrate how all the three dimensions of the Corporate Responsibility Matrix are interconnected and practically assisting the board in the implementation of corporate information governance. Figure 7.3 is used to explain how they function to facilitate understanding of the Modular Activity Plan.

The board directs the company by issuing directives, goals and objectives. These directives are cascaded down through the organisation and compliance to the goals and objectives is monitored at the different levels by means of performance measurements and deviation analysis. Any lack of compliance is reported back up the hierarchy and remedial action is taken, if deemed necessary.

The left hand side of the Modular Activity Plan constitutes the Directing function relative to each core aspect. Each level has a number of tasks or activities, which are used as a means of covering the major issues relative to that specific core aspect.

The right hand side of the Modular Activity Plan constitutes the Control-
7.5. **THE CORPORATE RESPONSIBILITY MATRIX**

![Modular Activity Plan Diagram]

Figure 7.3: Modular Activity Plan

ling side, again per level of management, illustrating the tasks and responsibilities needed to ensure that performance is measured, deviations analysed and reported back up the chain of command, to the board. Each core aspect has its own Modular Activity Plan to ensure the major activities of corporate information governance are included.

Each of the three dimensions of the Corporate Responsibility Matrix, namely: the Directing component (comprising of the four core aspects - Strategic Planning, Value Delivery, Risk Management and Resource Management), the Controlling component (comprising of Performance Measurement, Reporting and Deviation Analysis) and the Responsibility component (comprising of the four levels of the organisation - board of directors (BoD),
CEO, CIO, Unit Heads), are discussed further, to illustrate their relevance with regard to the corporate information governance process.

7.5.2 A. Directing Components

Information governance is a continuous cycle as illustrated in the process of corporate information governance in section 7.3. It generally starts with the setting of IT and IS strategy and its alignment with the organisational strategy. The implementation of these strategies occurs, ensuring the delivery of value that the strategies promised and addressing the risks that need mitigation. At regular intervals, compliance to the strategy needs to be monitored and the results measured, reported and acted upon. These strategies may need to be re-evaluated and realigned if and when appropriate.

The responsibility of the board for directing an organisation includes the setting of sound guidelines and objectives for the organisation with regard to the governance of the information asset. These need to be set for each of the four core aspects. Therefore, each core aspect will be discussed individually.

Core Aspect A1. Strategic Planning

This is one of the most important functions of the board and senior management. The development of a corporate information strategy is a complex process that generates the objectives and goals of the organisation in several major areas, such as IT and IS strategies, IT and IS infrastructure investment, organisational approach to IT and IS, corporate IS policies and programs, best practices and global risk profiling. The strategic plan is more than an inventory of funded application. It addresses steps to improve the technical infrastructure, ensures the provision of adequate resources for the information security efforts, defines cultural values relating to risk awareness, to ensure that the organisation is in a position to take advantage of identified opportunities (Glaser, 2004).

The board needs to take into consideration the following aspects when formulating their corporate information governance strategy (IT Governance Ltd, 2004a):

- Business objectives and competitive environment;
Current and future technologies, their costs, risks and any benefits which they can bring to the business;

The capability of the organisation and technology to deliver current and future levels of service to the business, and the extent of change and investment this implies for the organisation;

Compliance with relevant legislation applying to the information asset;

Creation of corporate information policies and programs, for example, a corporate information security program;

The cost of current information technology and information security and whether these provide sufficient value to the business;

Global risk profiling;

Best practices;

The relationships between the organisation and its stakeholders;

The lessons learned from past failures and successes.

An important aspect of corporate information Strategic Planning is the alignment of IT and IS strategies with the business strategies. The board needs to ensure that the investment of the organisation in IT and IS is in harmony with its strategic objectives and in doing so, the board ensures that the organisation is investing in capabilities, which, in turn, delivers business value. The board should direct this alignment by (Jennings, 2004) (IT Governance Institute, 2001):

Ascertaining that the IT and IS deliver against their respective strategies through clear expectations and measurement;

Directing IT and IS strategy to balance investments between supporting and growing the organisation and the agreed upon risk profile;

Making considered decisions about where IT and IS resources should be focused;

Ascertaining what security requirements are needed for the requirements of the organisation;
Figure 7.4: Modular Activity Plan for Strategic Planning
7.5. THE CORPORATE RESPONSIBILITY MATRIX

- Ensure that the security solutions are adequate for the processes of the organisation.

Figure 7.4 represents the Modular Activity Plan for the Core Aspect of Strategic Planning. It illustrates the different hierarchical levels of the organisation with their relevant activities and tasks. The left hand side of the plan indicates how the Strategic Planning for corporate information governance, is set at board level and cascaded down through the hierarchy, with the activities/tasks changing from governance functions to management functions. The creation of a corporate information security program is an important function of the board and indicates the commitment of both the board and senior management to information security governance (Whitman & Mattord, 2004).

The right hand side of the plan indicates how activities/tasks, relating to the Controlling function of the organisation, change from the unit heads level (management) upwards to the board. These tasks or activities of the Controlling functions include measuring of Performance, Deviation Analysis and Reporting tasks or activities.

“Doing the right things, and doing the right things right, requires executive agreement on what really are the right things.” (Senn, 2004).

Core Aspect A2. Value Delivery

Value has been defined as whatever contributes to current business goals and desired future goals (Thorpe, 1997). Value Delivery, with regard to corporate information governance, can be defined as concentrating on optimising expenses and proving the value delivered by IT and IS (IT Governance Ltd, 2004a). Expenditures, on both IT and IS, increase yearly, often without any obvious increase in return on investment. Both the actual costs and the return on investment need to be managed for effective value delivery to be achieved.

It was noted from the fundamental issues revealed in Chapter Six that the aligning of IT and IS strategies with business strategies leads to investment and business decisions that will enhance competitive advantage,
improve business processes, company reputation and profitability, and thus, deliver value to the organisation.

The increasing of the transparency of the organisational activities can add value to it by enhancing the trust between shareholders and the board; the customers and the organisation, but with increased transparency comes risk that needs to be managed appropriately.

The following means can used by the board to ensure that IT and IS deliver value (Jennings, 2004) (IT Governance Institute, 2001):

- By implementing a business strategy that focuses on providing an efficient, continuous service that meets the requirements of the organisation;
- Via a strategy for IT and IS that delivers on time, within budget and with the benefits that were promised;
- By outlining a corporate information security policy and practices that implement best practices;
- By properly prioritising and distributing efforts to the areas of the organisation with the greatest impact and business benefit;
- By implementing a continuous improvement culture relating to risk awareness.

Value Delivery can be measured by its financial worth, that is its contribution in monetary terms; its alignment, that is whether it is aligned with the organisational business goals; and lastly risk, that is the chance of not realizing the expected benefits (Thorpe, 1997).

Different levels of management and users perceive Value Delivery differently. Generally, it is easier to measure the impact of an IT investment at the lower levels than at the top of the hierarchy. For example, the cost per transaction is easily measured, but return on assets is more difficult to measure.

The Modular Activity Plan as illustrated by Figure 7.5 , has been proposed to ensure that the board can practically implement the core aspect of Value Delivery.
Figure 7.5: Modular Activity Plan for Value Delivery
The tasks/activities relating to this core aspect have been allocated to the different levels of the organisational structure and are delineated by the governance functions of Directing (left hand side of plan) and Controlling (right hand side of plan). The tasks/activities that need to be measured and monitored are described on the Controlling side, and the reporting aspects are highlighted.

**Core Aspect A3. Risk Management**

Risk is an uncertainty about a potential event or the possibility that a negative event is going to occur without an organisation being equipped to handle it. Risks, if not properly managed, can be harmful to a company and therefore, preventative measures need to be implemented through a process of Risk Management (Thomson, 2003b). Risk Management includes addressing the safeguarding of the information asset and business continuity by providing a disaster recovery plan (IT Governance Ltd, 2004a). The King Report (2001) places the responsibility for ensuring that there is a resolute system of Risk Management in place, within an organisation, squarely on the shoulders of senior management and the board. Risk Management is necessary to protect the assets of the organisation and to support business objectives according to good corporate governance principles. One of the main aims of Risk Management, within an organisation, is to avoid or lessen the impact of risks.

The 2002 Department of Trade and Industry Information Security Breaches Survey revealed that almost 95% of United Kingdom companies failed to meet their corporate governance duties to manage information risks (Rathmell, 2002). The need to provide effective corporate governance for shareholders and customers is the driver for increased Risk Management activities in organisations. Organisational risk is financial risk and includes operational and systemic risk, within which technology risk and information security issues are prominent.

There are risks involved in deploying certain technologies and in not deploying others. There needs to be a structured approach to risk assessment that generates a risk treatment plan where risks are accepted, controlled, eliminated or contracted out (IT Governance Ltd, 2004a). The mitigation of these risks is solved by embedding accountability into the company. Both risk assessment and risk mitigation need to be supported by adequate re-
sources to ensure success and measured to ensure that the required results are obtained. The Y2K problem showed how operational risk can create serious business risk (Institute of Internal Auditors, 2001).

The board should do the following to manage risk within an organisation (King Report, 2001):

- Be aware that the final responsibility for Risk Management is the responsibility of the board while management is accountable to the board for designing, implementing and monitoring the process of Risk Management and integrating it into the daily activities of the organisation;

- Set the risk strategy policies in liaison with the executive directors and senior management;

- Decide the tolerance or appetite for risk of the organisation, that is, decide those risks it will take and those it will not take in the pursuit of its goals and objectives;

- Consider that a transparent and proactive Risk Management approach can create competitive advantage.

Effective Risk Management starts with a clear understanding of the appetite of the organisation for risk, the understanding of the risk exposure and an awareness of the Risk Management priorities. Strategies for Risk Management can be set and responsibilities assigned once the risk appetite has been defined and the risk exposure identified. There are a number of ways in which the board can deal with risk. Risks can be allocated by using contracts and service level agreements. Risks can be mitigated by implementing internal controls by either acquiring or deploying security technology to protect the IT infrastructure. Risks can be transferred by sharing risk with partners or transferring to insurance coverage. The board can use risk assurance through audit and certification, or accept risk by formally acknowledging that the risk exists and monitor it (IT Governance Ltd, 2004a).

Figure 7.6 refers to the Modular Activity Plan relative to the Core Aspect of Risk Management and illustrates the different tasks/activities per level of organisation.

The tasks/activities relating to the board are governance issues while the other levels are management issues.
Figure 7.6: Modular Activity Plan for Risk Management
Core Aspect A4. Resource Management

The goal of resource allocation and management is to optimise the utilisation of IT and IS assets; lower the total cost of ownership; improve IT and IS investment decisions and ensure delivery of the promised value of computing by making the knowledge resources more productive (InfoSec, 2003). Technology should contribute to improving the following: productivity; customer service; supply chain management; cost control and shareholder information (IT Governance Ltd, 2004b). The board and senior management should strive to maximise the efficiency of their information assets and optimise the costs relating to these assets. Outsourcing has grown over the last few years, but this has brought its own problems. The board needs to decide where and how to outsource and should maintain a strict control over the management of the outsourcing services to ensure that the promised value is being delivered and the required level of security is being maintained.

The board should ensure that the IT and IS assets are organised optimally providing the required quality of service through the most cost-effective delivery infrastructure. Organisations that achieve this successfully can realise great cost savings and will be well placed to take on new IT and IS initiatives, introduce new emerging technologies and replace or update obsolete systems (IT Governance Ltd, 2004a).

Information technology and IS assets have always been difficult to manage because they change continually, due to the nature of technology itself and changing business requirements. The board needs to assure itself that effective management is in place to deal with the hardware, the software licences, the service contracts, the permanent and contracted people etc. and for managing changes, minimising service incidents while assuring a reliable quality of service.

The fundamental issues highlighted in Chapter Six, revealed that it was important for both IT and IS governance that the investments in technology and security be commensurate with its risks. The function of the board with regards to Resource Management and allocation needs to ensure that there is a balance between investment and risk. This, in turn, leads to the IT and IS assets being optimally utilized, an improvement in the decision-making process with regards to IT and IS and lastly, the lowering of the total costs of ownership.
Human resources, of all the organisational resources, represent an important part of the cost base and is the one most likely to increase. Thus, it is essential for the board and senior management to identify and anticipate core competencies that are required in the workforce. Once this has been achieved, an effective recruitment, retention and training program can be implemented ensuring that the organisation has the skills to utilize its IT and IS assets effectively to achieve its stated objectives, which is an important function of the board (King Report, 2001).

It is vitally important for both IT and IS governance, with regard to human resources, that education, awareness and training are provided. The programs for education, awareness and training need to be thoughtfully designed to encourage desirable organisational behaviours. It is equally important that the board and senior management are seen to be leading this shaping of the corporate culture, by playing an active role and “practising what they preach”. The board and senior management who are observed not following the management policies influence the employees, who observe their behaviour to determine how they should behave and will consequently also ignore the management policies. (Thomson, 2003b).

Figure 7.7 illustrates the Modular Activity Plan, which relates to the Core Aspect of Resource Management.

The Directing dimension of the Corporate Responsibility Matrix contain the four suggested core aspects that are important for the direction of the organisation, as far as the corporate information governance is concerned. There is a valid business axiom which states that “You cannot manage what you cannot measure”. Therefore, it is essential to ensure that after the strategies, policies and objectives have been filtered down through the organisation, there is a means of Controlling in place ensuring compliance to these strategies, policies and objectives. The Controlling component is discussed next examining the different means used by the organisation to measure and monitor its compliance to the objectives and goals set by the board and senior executives.
7.5. **THE CORPORATE RESPONSIBILITY MATRIX**

**Figure 7.7: Modular Activity Plan for Resource Management**

- **Core Aspect A4: Resource Management**
  - **BoD**: Monitor the latest IT & IS developments from a business perspective, compare the investment in IT & IS with other like organisations, monitor the major investments from a risk and return perspective, evaluate if suitable IT & IS resources, infrastructures and skills have met the required strategic objectives.
  - **CEO**: Brief the board on success of IT resource management, evaluate the cost of infrastructure assets with the quality of service required, evaluate the ability to retain skilled IT & IS staff, evaluate outsourcing opportunities, evaluate management of outsourcing contracts.
  - **CIO**: Evaluate how the organisation is leveraging its knowledge to increase stakeholder value, ascertain how the IT assets are being managed, evaluate that there are suitable internal IT & IS skills to manage and support their projects and systems, measure/reward individuals and team performance.
  - **Unit Heads**: Evaluate skills of staff to ensure the meeting of strategic objectives, monitor the efficient and optimal use of resources and increase the effectiveness of IT processes, evaluate staff productivity and morale, monitor compliance of staff to security policies, measure performance of actual vs budget.

- **A. Directing Function**
  - **Set policies on resources are needed to achieve strategic goals**
  - **Ensure a proper balance of IT & IS investments for sustaining and growing the enterprise**
  - **Set policies on outsourcing**
  - **Ensure investment into IT & IS are commensurate with risk appetite**
  - **Ensure organisation is in the best position to capitalise on its information and knowledge assets**
  - **Establish business priorities and allocate resources to enable effective IT & IS performance**
  - **Set up organisational structures and responsibilities that facilitate IT & IS strategic implementation**
  - **Build security conscious culture**
  - **Provide direction for sourcing and use of IT & IS resources**
  - **Allocate business resources required to ensure effective info governance over projects and operations**
  - **Balance investments between supporting and growing company**
  - **Direct IT & IS architecture design**
  - **Research technology for future growth**
  - **Oversee security education, awareness & training**
  - **Provide IT infrastructures that facilitate creation and sharing of business information at optimal cost**
  - **Ensure availability of suitable IT resources, skills and infrastructure to meet the strategic objectives**
  - **Define roles critical for driving maximum value from IT**
  - **Standardise architectures and technology**
  - **Educate and train staff to obtain required skills**
7.5.3 B. Controlling Components

A responsibility of the board is to retain full and effective control over the enterprise and they are required to monitor management in their implementation of their plans and strategies (King Report, 2001). It is recognised that the elements found in this section are essentially management functions, but they are included specifically to enable the inclusion of the Controlling activities in the Modular Activity Plans to ensure “full-cycle” governance.

B1. Performance Management

Performance management is a management system for defining, planning, measuring, analysing, reporting and improving the performance of the resources of the organisation. The objective of Performance Management is to ensure that performance targets and performance service levels are achieved through the effective and efficient use of systems resources (Frenzel, 1992).

Information technology performance and effectiveness are generally monitored using performance measures that indicate the efficient operation of an underlying control. Some examples include (IT Governance Institute, 2004):

- Defect identification and management - includes the establishing of metrics and analysing the trends of actual results against metrics and provide a basis for understanding the underlying reasons for processing failures;

- Security monitoring - an effective IT security infrastructure can reduce unauthorised access. Improving security can reduce the risk of unauthorised transactions and the generating of inaccurate reports and reduce the unavailability of key systems if there has been a security breach.

The saying “What gets measured gets done” is applicable here, as well as the converse - “What isn’t measured, is probably not being done”. Therefore, implementation of any important strategy must be regularly and continuously monitored ensuring the desired state is being met. The organisation needs to act upon the results of the monitoring. Either the compliance results are recorded for management reporting; or controls are changed to attain the goal-state; or the goal itself is changed (Moulton, 2004).
Organisations need to examine their information governance processes to identify how those processes are encouraging desirable behaviours and how they link to performance metrics. It is not enough for the board to ensure that IT and IS investment deliver value and enable the business, they must ensure that the investment encompasses what is necessary to mitigate any risks that may arise from their deployment. It is imperative that this occurs on a continuous basis.

As an organisation’s dependence on information technology increases, tolerance decreases for systems that are not secure, not available when needed and unable to produce accurate information on a consistent basis. An unreliable system, like a weak link in a chain, can cause a succession of events that negatively affect an organisation and its customers, suppliers and business partners (Institute of Internal Auditors, 2001).

**B2. Deviation Analysis**

Deviation analysis is implemented by asking the following question “If this”... “then what?” This is explained by the following example: Motor vehicles are supplied with a spare wheel. This statement illustrates an excellent action plan based on answer to the posed question. If this car has a flat tyre, what is the solution? Answer: Keep the spare wheel in the car.

This question is the base one asked to undertake deviation analysis or “gap analysis”, which is an essential tool in the overall governance of the information asset. The evaluation of the performance of any system requires that performance baselines be established. These are expected levels of performance against which all subsequent levels of performance are compared (Whitman & Mattord, 2003). The board should satisfy itself that plans for countering deviations from strategies and objectives are in place and are continuously updated keeping pace with a rapidly changing environment.

**B3. Reporting**

Reporting plays an essential role within the management system. Reporting is important within the organisation and to all its stakeholders. The sharing of information with all the stakeholders and consequently increasing transparency is important to any organisation because it has the ability to improve performance and build trust. The reporting of problems, failures
and successes exposes the individual and organisation to both criticism and praise. More importantly, open communication leads to an increase in trust and confidence that could ultimately have financial benefits to the organisation (Frenzel, 1992).

The implementation of adequate corporate information governance requires that roles and responsibilities need to be assigned. This forms the last dimension of the Corporate Responsibility Matrix and is discussed in the next section.

### 7.5.4 C. Responsibility Components

An important function of the board is to assign roles and responsibilities to specific people within the organisation, ensuring that accountability and performance can be measured and controlled. The use of the National Cyber Security Summit Task Force’s Information Security Governance Framework (National Cyber Security Partnership Governance Task Force, 2004), the BSA’s ISG Framework (Business Software Alliance, 2003) and the IT Governance Institutes’ Board Briefing on IT Governance (IT Governance Institute, 2003) have identified four different management groups as the major levels in an organisation with regard to the governance of information. The highest level includes the board of directors (BoD) denoted as C1, then the Chief Executive Officer (CEO) denoted as C2, the Chief Information Officer (CIO) denoted as C3 and finally, the Business Unit Heads or Unit Heads denoted as C4.

The board of directors takes a holistic view of the organisation and sets strategies and objectives. The CEO focuses on driving value down through the organisation ensuring the goals and strategies are communicated throughout the organisation and reinforces the corporate vision. The CIO co-ordinates across the organisation and identifies strategic technologies. The Business Unit Heads ensure compliance and give feedback. Each level plays a part and needs to be held accountable for their activities in the protection of the information asset. A part of the role of the CIO is to co-ordinate all these activities and ensure that dialogue between the board, the IT and IS departments and the rest of the organisation is continuous.
The two major functions of the board, Directing and Controlling (King Report, 2001) and the important function of allocation of responsibilities, were presented in the form of a three-dimensional matrix called the Corporate Responsibility Matrix (see Figure 7.2). The Directing function “A.” of the matrix consists essentially of four “core aspects” identified as A1 to A4 illustrated in Figure 7.2. The Controlling function “B.” consists of Performance Management, Deviation Analysis and Reporting, identified as B1 to B3 illustrated in Figure 7.2. The Responsibility levels (C1 to C4) are included in the matrix purely, to differentiate the involvement of corporate hierarchical levels. This Corporate Responsibility Matrix was developed to bring together all the different components that have been highlighted as important to corporate information governance during the literature study and to facilitate the development of the supporting Modular Activity Plans. The purpose of these Modular Activity Plans is to demonstrate clearly who is responsible for which functional activity and interconnects all three dimensions of the matrix. These Modular Activity Plans (MAPs) are a means that can be used by the board to practically implement an improved corporate information governance process.

### 7.6 Benefits of Implementing the Matrix

The potential benefits derived by organisations implementing this Corporate Responsibility Matrix and the Modular Activity Plans extend beyond facilitating compliance with applicable legislation, regulatory and contractual requirements. Some tangible business benefits include (Entrust, 2004a):

- Improved internal processes and controls, such as the authentication and authorisation of the employees, devices and applications on the network, the improved efficiency and effectiveness of business processes;
- The potential for lower audit and insurance costs due to better governance and the ability to demonstrate an auditable, complete corporate information governance framework that should result in lower insurance costs and decreased audit costs;
- Market differentiation through a continuous improvement process because the re-iterative framework should be regarded as a method for
improving productivity and customer loyalty;

- Self-governance is a better alternative than regulation because the framework is based on standards and best practices, which should mitigate the requirements for new governmental regulation.

An effective way to get started in implementing a proper information governance program is often to ask tough questions, but those responsible for the governance function will require adequate answers to these questions. It is essential to determine not just the action, but also **who** is responsible to deliver **what** by **when**.

An effective action plan should be implemented by the board and could include steps to (IT Governance Ltd, 2004a):

- Set up a governance organisational matrix and Modular Activity Plans, such as the Corporate Responsibility Matrix suggested in this dissertation, which will enable the governance of the information asset to go forward with clear roles and responsibilities and objectives identified ensuring the achievement of these objectives;

- Align IT and IS strategy with business goals by ensuring that the board has a good understanding of the business environment, risk appetite and business strategy;

- Understand and define the risks by considering previous history and patterns of performance of current IT and IS organisational factors, the complexity and size or scope of the existing and planned IT and IS environment and the nature of the IT and IS initiatives being considered;

- Develop improvement strategies by deciding which projects will help in improving the management and governance of these significant areas.

There are many benefits to implementing effective corporate information governance, as previously stated. It is vital that the board take cognisance of the fact that they are responsible for the adequate governance of the information asset of the enterprise. The lack of adequate corporate information governance could have serious consequences for the organisation, its shareholders and other stakeholders and for the board, who could face personal,
legal and/or criminal liabilities for inadequate and ineffective corporate information governance.

7.7 Conclusion

The purpose of this dissertation is to identify the reason or reasons why many corporate disasters and losses have been attributed to poor governance of the information asset and to propose a means for improving corporate information governance.

Some of the reasons for this reported inadequate governance, as established by the literature studied, are:

1. A lack of expertise and knowledge surrounding the information asset, exists at board level and consequently;

2. The board has tended to leave this important function to management to cope with, while at the same time, limiting the amount of capital available with which to manage the asset adequately;

3. There are inequalities prevalent in terms of the division of available funds between information technology and information security;

4. It appears that the board is not always fully aware of the real governance activities required for the proper governance of the information asset.

The above findings have been reported on in Chapters Three, Four, Five and Six and fulfill part of the requirement for achieving the objectives of this dissertation.
Chapter seven fulfills the objectives of the dissertation by:

1. Clearly identifying the four suggested core aspects of corporate information governance, namely, Strategic Planning, Value Delivery, Risk Management and Resource Management;

2. The linking of important fundamental issues to their appropriate core aspects;

3. The formulation of a Corporate Responsibility Matrix (see Figure 7.2), which endeavours to highlight who has Responsibility for which information governance aspect. The management functions of Performance Measurement, Deviation Analysis and Reporting are included to close the recommended governance cycle;

4. The providing of four Modular Activity Plans, each addressing a core aspect, providing specific recommended activities/tasks, which, if properly implemented will improve the governance of the vital information asset.

Corporate information governance is an essential component of corporate governance that addresses the process of information governance. This process has been sadly lacking in many organisations. This chapter has set out practical means for implementing an improved process for information governance and has included the two basic functions of governance - Directing and Controlling - incorporating Responsibilities delegation to different levels of management to ensure accountability.

Adequate and effective information governance is an essential function of the board and this can be achieved through implementing all the dimensions of the corporate responsibility matrix in conjunction with the practical implementation of the Modular Activity Plans for each Core Aspect.

This is the penultimate chapter of this dissertation and a summation and conclusion chapter follow.
Part IV

Conclusion
Chapter 8

Conclusion
8.1 Introduction

Corporate governance systems have evolved over many decades, as the result, inter alia, of the continuous need to increase returns on investments in an ever more competitive market-place.

Information has always played an important role in corporate governance and the advent of computing power has elevated information, per se, to a position as one of the most vital assets of an organisation (Institute of Internal Auditors, 2000a).

The literature indicates that the governance of the information asset has unfortunately not “kept pace” with the exponential growth of the information asset. This has, allegedly, led to some serious corporate losses and in some instances corporate failures.

This dissertation set out to study the governance of the information asset to identify the reasons for the reported corporate losses/failures attributed to the inadequate governance of the information asset. Additionally it sets out to include proposals for the improvement of the governance of this asset as derived from the study results.

The following section contains a summary of the material explored in the previous chapters.

8.2 Summary

The opening chapter of this dissertation introduces corporate governance, with particular reference to the governance of the information asset. There have been frequent reports of corporate disasters, some of them allegedly due to poor information governance and the area of study was defined and questions were raised related to the reasons for this allegation. The problem statement was defined and the primary objective of determining whether these allegations were correct and how to set about improving the governance of the information asset was defined with supporting secondary objectives. The methodology for achieving these objectives includes a comprehensive literature study, arguments and models.

Chapter Two reviewed several corporate failures/losses and highlighted some corporate “sins”, pointing out the disastrous impact these could have
on corporations and their stakeholders. Chapter Two further expounded on
the relationships between information, organizational structures and inform-
ination governance. A brief history of corporate governance, its functions
and its importance was presented. An insight was provided into the roles
and responsibilities of corporate boards, vis-à-vis, their responsibilities for
the governance of the information asset. The concept of a subcomponent of
corporate governance with oversight of the information asset, by the board,
was introduced.

Chapter Three proposed a definition of corporate information governance
as a focus subject. It was deduced by posing insightful questions, that the
subject, corporate information governance, should be divided into two com-
ponents for study purposes.

The reasons why these two components should be considered as gover-
nance issues were introduced and one of the common elements, risk was
highlighted. This chapter closed by proposing a structure for corporate in-
formation governance responsibilities, enabling the information asset to be
elevated to the board as a specific governance responsibility.

Chapter Four concerned itself specifically with the first identified study
component of corporate information governance, namely the governance of
information technology. This chapter initially concentrated on an overview
of the information technology asset. Information technology was defined and
its rapid growth and the expansion of this asset into most areas of the cor-
porate environment was highlighted. The literature study further revealed a
paradox that despite very large investments (with ensuing risks), information
technology has not met the expectations desired of it.

It was noted that despite the undoubted importance of IT in the cur-
rent corporate world, one of the major reasons for these failures is a lack of
attention to IT by senior executives and the board.

This led directly to a discussion of the governance of this important asset
of the organisation. It highlighted the responsibilities of the board with re-
gard to information technology and discussed some of the important strategic
issues that needed to be dealt with. The overall objective of the governance
of information technology was examined and its purposes. There was a need
to clearly define an IT governance process that needed to be implemented by
the board to achieve this objective. This process was discussed to discover
what it entails. It was consequently argued that there is a definite need for
the governance of information technology to be elevated to board level.

Chapter Five initially concerned itself with providing a background de-
scription of information security, the second identified study component. In-
formation security was defined and its various characteristics were discussed,
illustrating that there are more than the generally accepted characteristics of
confidentiality, integrity and availability involved. It was argued that infor-
mation security equally needed to be elevated to board level with oversight.
The issue of compliance was discussed illustrating some of the serious conse-
quences of non-compliance. The second section of Chapter Five delved into
the subject, the governance of information security and, once again, sev-
eral important areas of direct concern for the board were highlighted. The
chapter drew the conclusion that the governance of information security is
equally as important as the governance of information technology and that
both form basic pillars constituting corporate information governance.

At this point in the dissertation, having argued the necessity for direct
board governance of both information technology and information security
from Chapters Four and Five, it was apparent that many similarities existed
between the two components.

Chapter Six explored the relationship between the governance of informa-
tion technology and the governance of information security, and the concepts
of “core aspects” and “fundamental issues” were subsequently introduced.
These core aspects, namely strategic planning, value delivery, risk and re-
source management form the groupings under which fourteen “fundamental
issues”, constituting the major issues and extracted from Chapters Four and
Five, were placed. The application of pertinent questions to each of the fun-
damental issues and by answering these questions with extracts from relevant
chapters, certain conclusions could be drawn. Key amongst these conclusions
were:

1. Both the governance of information technology and information secu-
   rity are equally important as governance issues;

2. Both should become board oversight issues;

3. An improved governance of the information asset could be achieved by
   implementing programs based on the findings of this dissertation.
8.3. THE PROBLEM AND ITS SOLUTION

The above conclusions meaningfully contribute to the achievement of the secondary objectives, as stated in Chapter One.

Chapter Seven draws from all the findings of the earlier chapters and proposes the development of a model, called the Corporate Responsibility Matrix. This matrix is a three-dimensional matrix combining the two major functions of the board, Directing and Controlling and links these to the assignment of roles and responsibilities at different levels of the organizational hierarchy. The objective of developing this Corporate Responsibility Matrix is the promotion of an optimized process for the governance of the information asset. The dimension of the matrix, relating to the directing component, comprises four core aspects introduced in Chapter Six. These core aspects are discussed in detail enabling the board to fully understand these important aspects for the purpose of facilitating the improvement of the governance of the corporate information asset. All three dimensions are combined and illustrated with the use of the Modular Activity Plans. These Modular Activity Plans indicate the tasks/activities of all four levels of the organisational hierarchy related to each core aspect, indicating the directing functions and the controlling functions separately. The purpose of these Modular Activity Plans is to assist the board to practically implement an improved corporate information governance process.

8.3 The Problem and its Solution

The problem statement of this dissertation stated that many corporate losses or failures have been cited as being caused by inadequate corporate governance of the information asset. Careful examination of the literature available on this subject has, indeed, confirmed the validity of this allegation (Changepoint Corporation, 2004).

The confirmation of the problem statement does not, however, provide a solution. A further in-depth study of the literature revealed a number of causative problems, directly related to inadequate governance of the corporate information asset. They include:

1. A lack of appreciation of the importance of the information asset by the board;
2. A lack of technical expertise at board level;

3. The inequities in the allocation of assets for and within the information asset;

4. An inadequate responsibility structuring for this asset;

5. A lack of reliable performance measurement and reporting mechanisms for this asset;

6. A lack of direct board representation for this valuable asset.

The solution for the problem statement rests on solutions for the causative problems and the following has been proposed:

- The promotion of an individual who has high level skills in information technology and information security, business management and sound communication skills to an executive seat on the board of directors, thus highlighting the importance of this asset at board level. This responsible individual must be given the authority needed to ensure the attainment of the corporate goals for the information asset. This will allow for the redress of inequities that could be existent in the allocation of assets for and within this critical asset;

- The employment of the Corporate Responsibility Matrix in order to ensure that roles and responsibilities are correctly allocated throughout the corporate hierarchy and to ensure that performance evaluation and corrective action where necessary is practiced by all responsible parties;

- The implementation of the Modular Activity Plans as proposed will clearly enhance the ability of the board and the CIO to implement adequate and effective corporate information governance by clearly identifying the tasks/activities related to each level of the organisational hierarchy in both areas of Directing and Controlling.

It is believed that the implementation of the above proposals will contribute to an improved governance of the corporate information asset, thus meeting all the objectives set out in Section 1.4.
8.4 Perceived Achievements of this Project

This dissertation set out to investigate the governance of the corporate information asset. It illustrated that there are some serious problems in the way many companies secure their information and govern their technology. It defined a term Corporate Information Governance which encapsulated both the information technology and the information security governance functions. In doing so, this project succeeded to illustrating the importance of each function and validating that both these functions should be treated as governance functions. Other achievements of this project includes the designing of a corporate information matrix, which showed the different dimensions of governance, namely controlling, directing and responsibility components, and how they interlinked with the core aspects of the different dimensions. From this matrix design, a series of modular activity plans were developed to facilitate the effective implementation of corporate information governance.

8.5 Perceived Limitations of this Project

Due to the lack of time, the modular activity plans have not been expanded upon to show how the various points should be approached and implemented by the different levels of management within the organisation. Neither was any evaluation done to determine their completeness or validation of the proposed plans in a practical context.

8.6 Further Research

The board needs to ensure that there is adequate governance of the information asset within their organisation. This is not easily achieved. This dissertation has merely investigated two components of corporate information governance, namely information technology governance and information security governance. Further research will address other aspects that could be associated with information governance.

Another area that can be addressed for further research is the design of the Modular Activity Plans that were created in this dissertation. The design of
these Modular Activity Plans are only described at a very high level. It is believed, that a positive contribution could be achieved by further research on a more detailed, implementable outline for each Modular Activity Plan for improving the governance of the information asset. Further research needs to be made to determine the completeness of the modular activity plan items at each level, and to validate their implementation in a practical context.

8.7 Conclusion

The governance of the vital information asset of an organisation is not an easy task. There have been many organisational disasters due to the lack of adequate corporate governance of this asset. The consequences of this lack of corporate information governance are very serious for the organisation, the board, shareholders, employees and customers.

It would be beneficial for the board to implement a framework that would facilitate the governance of the information asset to rectify this situation. This has been achieved with the development of the Corporate Responsibility Matrix along with the Modular Activity Plans. The purpose and objective of these models is to practically assist the board in implementing an improved corporate information governance process. This will greatly aid these organisations from repeating the same disasters presented in Chapter Two.
References


REFERENCES


Glaser, J. P. (2004). The mystery of IT strategy: strategy failures present one of the greatest risks to a significant information technology investment. Available from: http://www.findarticles.com/p/articles/mi_m3257/is_1_58/ai_n6068618.


REFERENCES


King Committee on Corporate Governance. (2002). *The Executive Summary of the King Report 2002*.


REFERENCES


Part V

Appendices

This paper outlined the important role of the board to adequately and effectively govern the information asset of a corporation. The paper highlighted the relevant aspects of corporate information security governance and set out a number of questions that should be addressed by the board regarding the governance of the information asset.