Corporate Information Risk: An Information Security Governance Framework

by

Shaun Murray Posthumus

Corporate Information Risk: An Information Security Governance Framework

by

Shaun Murray Posthumus

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: Professor Rossouw von Solms

January 2006

Declaration

I, Shaun Murray Posthumus, hereby declare that:

- The work in this dissertation is my own work.
- All sources used or referred to have been documented and recognized.
- This dissertation has not previously been submitted in full or partial fulfillment of the requirements for an equivalent or higher qualification at any other recognized educational institution.

Shaun Murray Posthumus

Abstract

Information Security is currently viewed from a technical point of view only. Some authors believe that Information Security is a process that involves more than merely Risk Management at the department level, as it is also a strategic and potentially legal issue. Hence, there is a need to elevate the importance of Information Security to a governance level through Information Security Governance and propose a framework to help guide the Board of Directors in their Information Security Governance efforts. IT is a major facilitator of organizational business processes and these processes manipulate and transmit sensitive customer and financial information. IT, which involves major risks, may threaten the security if corporate information assets. Therefore, IT requires attention at board level to ensure that technology-related information risks are within an organization's accepted risk appetite. However, IT issues are a neglected topic at board level and this could bring about enronesque disasters. Therefore, there is a need for the Board of Directors to direct and control IT-related risks effectively to reduce the potential for Information Security breaches and bring about a stronger system of internal control. The IT Oversight Committee is a proven means of achieving this, and this study further motivates the necessity for such a committee to solidify an organization's Information Security posture among other IT-related issues.

Acknowledgements

I would like to thank Professor Rossouw von Solms for the time, valuable insight and guidance that he provided without which this dissertation would not have been possible. Additionally, I would like to thank the National Research Foundation for the funding that they provided which enabled this task to be completed with ease.

Contents

List of Figures

Part I

Introduction

Chapter 1

Introduction

1.1 Background

Terry Simister, Chairman of the Institute of Risk Management (IRM), opined that the term risk management was coined as early as 1950's (Simister, 2000). Insurance managers began to identify themselves as risk managers during this time and began practicing what they termed as risk management activities. Simister (2000) further illustrates that the term risk management became the latest buzzword and gained immense popularity. Shortly thereafter, risk management activities became widely utilized largely by insurance underwriting and broking disciplines to deal primarily with financial risks. Over time, more disciplines, including Information Technology (IT), began to realize the benefits of applying various risk management practices to their day-to-day business activities and this saw the expansion of risk management into a formally accepted and renowned discipline (Simister, 2000).

Risk management is no longer used purely in the financial sense, therefore it is necessary to define exactly what this process entails, as many disciplines have their own understanding according to Simister (2000). Cule, Schmidt, Lyytinen, and Keil (2000) assert that "while we can never predict the future with certainty, we can apply structured risk management practices to peek over the horizon at the traps that might be looming, and take actions to minimize the likelihood or impact of these potential problems". The objective of the risk management process can be defined as recognizing and reacting to every potentially harmful risk through the planning, arranging and controlling of various activities and resources to dissipate the criticality of these risks

to a more acceptable level. This is achieved through the implementation of a risk management strategy that satisfies the risk appetite of an organization.

1.2 Description of the Problem Area

Most organizations today rely on the wide use of IT to execute their various business operations. This has brought about the realization of a vast number of additional risks that must be addressed. These risks require the implementation of various IT risk management strategies. Risks, from the IT perspective, comprise the three characteristics of assets, threats and vulnerabilities (Gerber & von Solms, 2001). Risk management, from the IT focus, is on the mitigation of these risks to a more acceptable level by either reducing the vulnerability or reducing the probability or impact of a threat to an asset.

Information technology risk management has been transformed overtime, by the changing nature of the IT environment to remain effective whilst dealing with the most recent security risks. Gerber and von Solms (2001) state that initially, computers had limited capabilities. These computers were large centrally located mainframes that processed data from various organizational departments. Risks were managed through simple physical security controls. Burglar alarms, burglar bars, security guards, surveillance cameras and locked doors are examples of such physical controls (Schneider & Perry, 2001).

The progression to distributed computing systems occurred through advances such as multiprocessing and high-speed communications. This made both hardware and software resources more accessible to computer users in remote locations, allowing them access disparate sites (Flynn & McIver McHoes, 1997). However, new risks came with these technology developments. Therefore, technical controls were introduced to mitigate the consequences of potential risks and included mechanisms such as access control, user authentication and data encryption (Gerber & von Solms, 2001).

Later IT began to facilitate both organizational business processes and services to business partners and customers. The Internet enabled many organizations to conduct business more conveniently through e-commerce. IT had begun to play an integral role in the daily operations of most or-

ganizations. The effective use of information was key to sustaining these organizations and consequently ensuring its protection was paramount. Consequently, there was a shift in the emphasis of what required protection. It was still important to protect the IT infrastructure but it had become more important to ensure the protection of information assets. This required the introduction of new types of security controls.

Gerber and von Solms (2001) illustrate that various operational security controls were introduced in the form of policies, standards and procedures. These enforce the adherence to certain codes of conduct and common security practices by users when using information systems. ISO/IEC TR 13335-1 (2004) and ISO/IEC 17799 (2005) are examples of such standards. The requirements for the security of information assets had by this stage become based on three distinct criteria. These criteria include firstly, requirements to protect the IT infrastructure; secondly, legal, regulatory and statutory requirements and thirdly, requirements for information integrity, confidentiality and availability (ISO/IEC 17799, 2005).

It now appears that the protection of business information requires more than merely ensuring that the technology by which it is managed, stored and communicated remains secure. Birman (2000) claims that security is more than a technical issue, it is also a strategic and potentially legal one. The Corporate Governance Task Force (2004) states that the road to Information Security goes through Corporate Governance and that although Information Security is viewed as a technology issue, it is equally a governance challenge that involves risk management, reporting and accountability on the part of executive leadership. In the past, Executive Management and the Board of Directors (BoD) were concerned with the management of financial risks. Information risks have now gained prominence due to the critical success factor of information.

In this information driven age strategic decisions are made based on business information and, therefore, Executive Management and the BoD need to be aware of and be held accountable for managing the risks that could compromise the security of information. Traditionally they deal with risks through the creation of policies and internal controls that direct and control the organization (Corporate Governance Task Force, 2004). These policies and internal controls constitute the organizational Corporate Governance

program and should include consideration for the protection of information. Such consideration would be best demonstrated through the creation of an Information Security Governance framework (Corporate Governance Task Force, 2004). This would demonstrate a commitment by Executive Management and the BoD to strengthening their Information Security posture and is more proactive in the management of all pertinent aspects of enterprise risk. There is a definite need to integrate Information Security into Corporate Governance. The Corporate Governance Task Force (2004) states that both risk and risk management are core to Corporate Governance, and that it is important to study risk and risk management in order to establish an effective Information Security Governance framework in order to successfully address business information risk.

As dependence on IT to facilitate business operations and deliver timely and accurate information increases, the criticality of IT becomes a fundamental business concern. Thus, effective Information Security Governance requires that IT be effectively addressed at board level as well. This is to ensure that the implementation and utilization of important technology resources are appropriately governed and their risks mitigated. For this reason IT Governance needs to become a key function of Corporate Governance and responsibility of the BoD. However, the Scottsdale Institute (2001) states that the BoD lacks the skills and insight necessary to effectively strategically direct and control IT. Usually, board-level committees are tasked with the responsibility of informing the BoD on more specialized matters like the Audit Committee on the organization's financial aspects. Therefore, the institution of an IT Oversight Committee will help advise the BoD in terms of IT Governance, IT-related risks and other strategic IT issues, and thereby bring about a stronger system internal control and an enhanced approach to Corporate Governance that fully enables the protection of important business information assets.

1.3 Problem Statement

Since IT is widely used to manage valuable business information, there is a need to protect information through various risk management and governance efforts. IT risk management is, however, hardly adequate to provide

enough security for business information because the scope of its protection encompasses more than IT alone. There is a dearth of appropriate information regarding business information risk because few models and guidelines exist. Kwok and Longley (1999) suggest that a major factor in data security management is modeling and documentation. Risk management efforts in IT are well established but this is not equally applicable to the management of business information risk.

The primary research question for this dissertation is: "What steps are needed to create an effective Information Security Governance framework that can be integrated into the overall Corporate Governance program and ensure that the BoD is able to make well-informed decisions relating to IT to address all aspects of business information risk effectively?"

The problem requires decomposition into smaller sub-problems to accurately address these issues. After careful consideration the following questions were raised:

- What does the process of risk management as it relates to information protection entail?
- What are the legal requirements relating to the protection of information?
- What are the organizational business requirements for the protection of information with specific regard to its security?
- What information regarding the protection of business information, be presented to Executive Management and the BoD to help them effectively address business information risk management issues?

1.4 Objectives

The primary objective of this study is to develop an Information Security Governance framework that will provide information risk related information into the Corporate Governance framework and demonstrate the importance of the IT Oversight Committee to advise the BoD on matters of IT and IT-related information risks. This will provide the BoD and Executive

Management with the relevant information to effectively govern information-related risks.

A number a secondary objectives need to be accomplished to achieve the primary objective. These are:

- The positioning of information-related risks within the broader risk management framework;
- The relation of information risks to IT risks;
- The recognition of a means to identify risk related information which will assist in the governance of IT risks.

1.5 Methodology

The methodology of the study involves an in-depth literature survey focusing on the field of Information Technology and Information Security. Through the literature survey various issues involved in the management of business information risk are addressed. The aim is to reinforce the argument that current IT risk management methodologies are insufficient to provide complete protection for business information. A model illustrating the requisites for meaningful reporting on the relevant issues of business information risk to the BoD is developed and the importance of an IT Oversight Committee to advise the BoD in IT matters is argued. This enables the integration of an effective Information Security Governance framework into the overall Corporate Governance program of an organization.

1.6 Layout

The dissertation consists of 8 chapters. **Chapter 1**, this chapter, presents the subject area of the study, the principal research question and further highlights how this question is addressed. Hereafter, **Chapter 2** discusses the concept of risk, risk management in general and Corporate Governance to demonstrate the importance of risk management as a Corporate Governance responsibility to ensure that shareholder interests are upheld. Risk management has a significant IT component and, therefore, IT risks should

be managed through proper IT risk management which is discussed in depth in **Chapter 3**. IT Risk Management plays a major role in Information Security which is important to protect information from IT as well as other risks. Information Security is demonstrated through effective Information Security Management which is addressed in **Chapter 4** and emphasizes the criticality of business information which requires board-level attention. This demonstrates the need for Information Security Governance which is discussed in **Chapter 5**. Information Security Governance requires that IT must be effectively addressed at board level as well. This is best accomplished through effective IT Governance which is explored in **Chapter 6**. Good IT Governance requires that the BoD make well informed decisions with relation to IT which, therefore, requires board-level IT oversight. IT oversight is discussed in **Chapter 7** to demonstrate its importance in facilitating Information Security Governance and IT Governance to remain effective in the preservation of critical business information assets by enabling sound decision making. **Chapter 8** summarizes the dissertation, highlights the final conclusions and presents further research possibilities. Figure 1.1 illustrates the layout of the dissertation.

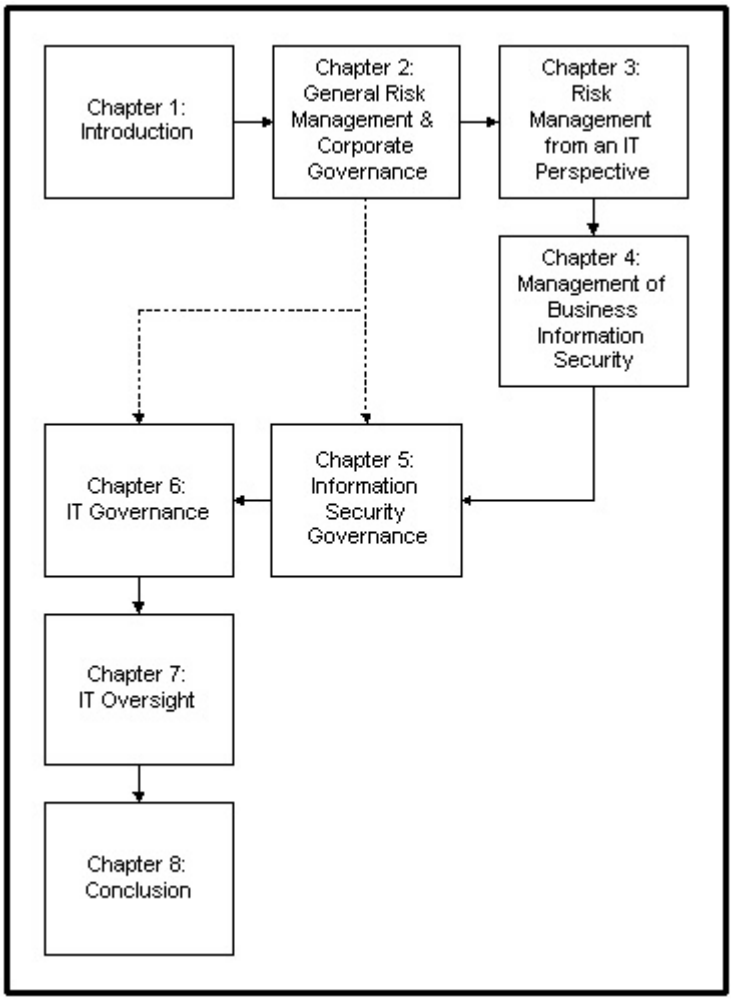


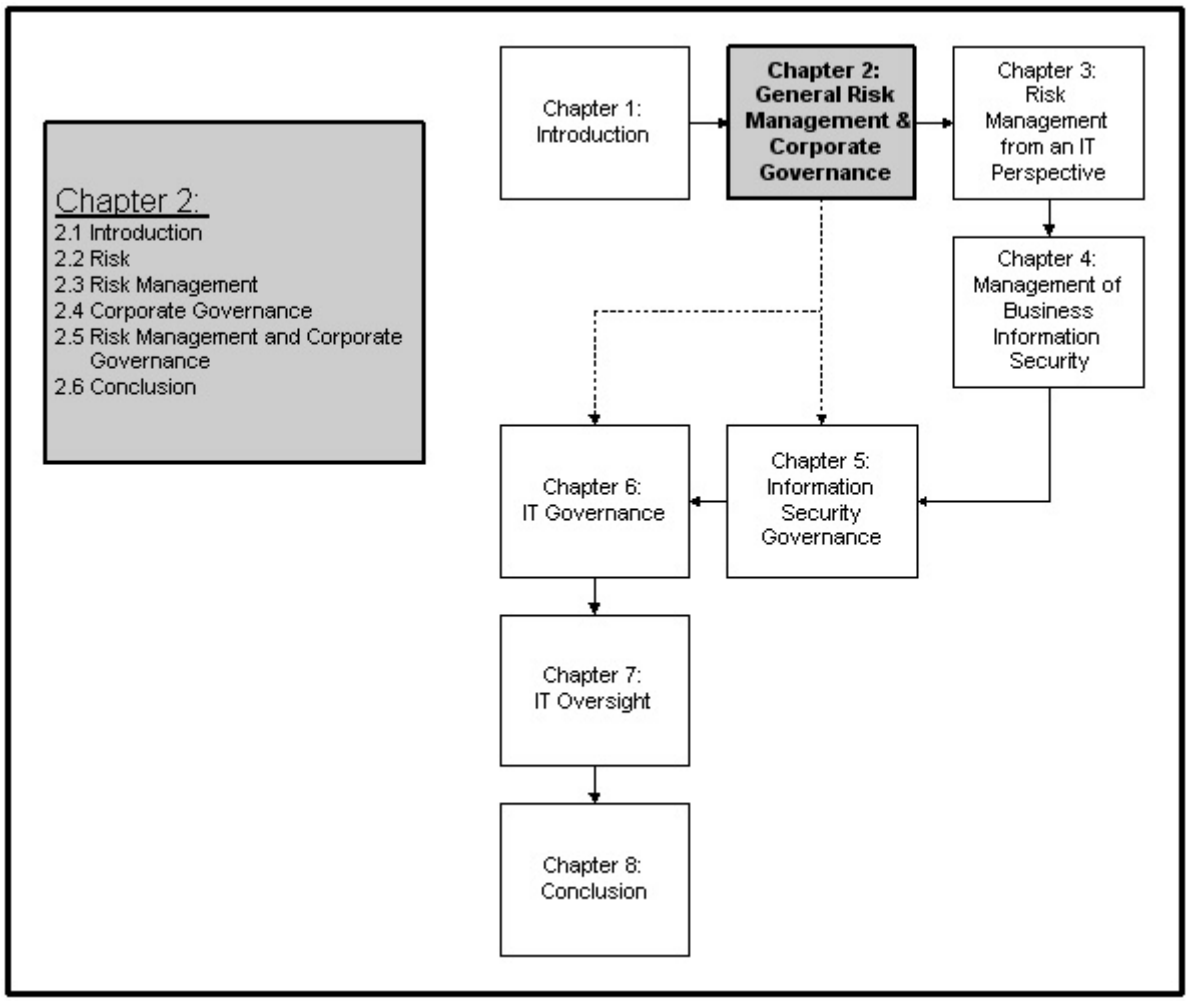
Figure 1.1: Proposed layout of the dissertation

Part II

Background

Chapter 2

General Risk Management and Corporate Governance



2.1 Introduction

This chapter discusses the concept of risk in general terms, highlighting a variety of perceptions in the various scientific domains. It examines various key areas of risk with the potential to impact upon individuals and society. Various means of controlling risks are explored, with this consideration it is noted that Risk Management is the most commonly executed function. Risk Management is discussed and various strategies of implementation are highlighted.

Risk Management is an important organizational function because it ensures the preservation of shareholder interests by reducing the risks that may prevent them from receiving adequate returns on their investments. It is the responsibility of the Board of Directors (BoD) to ensure that the shareholders interests are considered. This is best addressed through the organizational Corporate Governance function, which is examined in more detail. The relationship between Risk Management and Corporate Governance is discussed to highlight the importance of Risk Management as a Corporate Governance function and the responsibility of the BoD. The BoD should be aware of their Risk Management responsibilities as part of their Corporate Governance duties, ensuring the stakeholders interests are adequately and effectively preserved. The BoD's responsibilities in terms of Risk Management are further discussed. This chapter highlights the importance of understanding where the most important organizational risks lie to meet shareholder expectations and produce business value in the current dynamic corporate environment.

2.2 Risk

The concept if risk is not new. Man has, since the beginning of time, been aware of the risks surrounding him. Risk is an extremely large and complex issue and its meaning has been central to many a debate between scientists in their various disciplines and fields of expertise (Frosdick, 1997). The concept of risk should be scrutinized to gain a better understanding as to why there is such debate over what appears to be a fairly straightforward topic.

2.2.1 What is Risk?

The meaning of the term risk has evolved over a very long period of time, and its development has been elaborated upon by Douglas (1990), starting approximately in the seventeenth century until the current date. In the seventeenth century the concept of risk was derived from the mathematics associated with gambling. During this time, it was perceived to mean probability combined with the magnitude of possible gains and losses. During the eighteenth century, however, risk began to acquire a more of a neutral connotation because it was perceived to take account of both possible gains and losses. Risk, in this sense, was initially employed by the marine insurance industry during this time period. Later still, during the nineteenth century, the concept of risk had begun to emerge in the study of economics. During this time the perception of risk by the general public had made them risk averse and consequently special incentives were required to attract entrepreneurs to investments that involved risk. In the twentieth century, and currently, the concept of risk is perceived as a mostly negative outcome, especially in engineering and science, where hazards are posed by modern technological developments in the petro-chemical and nuclear industries (Frosdick, 1997).

Today, however, there still remains much confusion and ambiguity over what risk actually means. Natural and social scientists continue to disagree on the subject having developed their own understanding and perceptions (Frosdick, 1997). The meaning of risk in each of these areas will be explored to determine some common ground amidst all of the debate and confusion that exists.

2.2.2 Defining the Concept of Risk

The Royal Society (1992) defines risk as "the probability that a particular adverse event occurs during a stated period of time, or results from a particular challenge". Furthermore, the Royal Society's 1992 report recognized the needs of engineers and scientists specializing in the study of risk (Frosdick, 1997). They included a definition from British Standard 4778, which classifies risk as "a combination of the probability, or frequency, of occurrence of a defined hazard and the magnitude of the consequences of the occurrence" (British Standards Institution, 1991).

Frosdick (1997) suggests that a distinction be made between individual risks and societal risks due to the different perceptions each of these imply. The Health and Safety Executive defines an individual risk as "the risk to any particular individual, either a worker or a member of the public, [that is] anybody living at a defined radius from an establishment, or somebody following a particular pattern of life" (Health and Safety Executive, 1988). Societal risks, which represent risks to society at large have been classified as "measured, for example, by the chance of a large accident causing a defined number of deaths" (Health and Safety Executive, 1988). Warner (1993) indicates that scientists and engineers use these definitions because they form the foundation of their practical work. This work entails assigning numbers to risk, derived from the calculation of probabilities and the use of information on failures and reliability (Frosdick, 1997).

To gain a better understanding of risk in the various sciences, and more specifically the natural and social sciences, it should be elaborated upon in more detail. Gerber and von Solms (2005) have revealed that these "sciences" constitute two of the three fundamental paradigms of scientific study.

The natural sciences paradigm, of which the engineering discipline forms a part, describes the assessment of risk as based on "objective scientific analysis" (Mayo & Hollander, 1991). Frosdick (1997) elaborates on this point, stating that "the engineering paradigm is one of quantification". It employs techniques which make quantified comparisons concentrating on technological risks rather than on human risks (Gerber & von Solms, 2005). Burnie (2003) states that the natural sciences paradigm relies on a systematic approach, i.e. a scientific method, which is derived from objective analysis instead of individual opinion. Kirkwood (1994) emphasizes this by stating that the objective evaluation of risk is non-judgmental. Such an evaluation would follow some defined and structured approach free from opinion. This is the fundamental difference distinguishing the natural from the social sciences (Gerber & von Solms, 2005). Risk, in the natural sciences, is perceived as an objective, measured value based on some scientific assessment or method of quantification. This is clearly evident considering the definitions provided by the Royal Society (1992), because they contain language such as "frequency" and "magnitude" which both denote measured values.

Risk in the social sciences is evaluated by "subjective public perception

based on values, belief and opinion, which are influenced by factors such as history, culture, politics, law and religion" (Gerber & von Solms, 2005). Furthermore Kirkwood (1994) motivates that subjective or perceived risks are determined without any scientific means and utilize qualities such as experience, judgment and ingenuity to arrive at decisions regarding whether something is indeed a risk. This contrasts with the natural sciences which base the perception of risk on some method of scientific assessment. Social scientists believe that "there are serious difficulties in attempting to view risk as a one dimensional concept" when "a particular risk or hazard [means] different things to different people in different contexts" and "risk is socially constructed" (Royal Society, 1992). This suggests that social scientists find it impractical to use a structured methodology to scientifically analyze and quantify risk when there are so many different determinant risk factors. Slovic (1991) suggests some of these factors may include aspects like familiarity and dread, when risk is perceived as an individual construct.

Today risk is viewed more as an individual construct in a more individualist global culture and has, therefore, progressed to mean accountability or liability for the occurrence of some event i.e. "in a more individualist global culture, being at risk means that society is out of sync with the individual, whose rights are in need of protection" (Frosdick, 1997). Douglas (1992) states that "a generalized concern for fairness has started us on a new cultural phase. The political pressure is not explicitly against taking risks, but against exposing others to risk." Therefore, governments worldwide have passed many laws and regulations to achieve this. These laws and regulations aim to protect the rights of individuals in terms of their personal safety and privacy through the delegation of accountability and responsibility for the occurrence of various events. They emphasize the need for risks to be brought under control. Priest (1990) suggests that the controlling of risks forms the fundamental basis of modern civil law.

There is an understanding of risk that is common to each of the domains of scientific study, despite their contrasting perceptions and definitions. This understanding is that risk is perceived from a negative point of view. Therefore, it is important to understand where potential risks may occur to ensure that all aspects have been covered and the most salient are managed to a level that is more acceptable.

2.2.3 The Key Areas of Risk

It is clear that the identification and appraisal of risks in the various scientific domains depends heavily on how risks in these areas are perceived. Williams, Smith, and Young (1998) suggest that there are several sources from which risks are generally perceived to occur, despite these differences in perception. These sources of risks stem primarily from seven general environments including the physical, social, political, operational, economic, legal and cognitive. Tchankova (2002) elaborates on each of these in more detail.

In the ***physical environment***, sources of risk stem from events such as natural disasters. These include earthquakes, storms, landslides, floods or tsunamis for example (Tchankova, 2002). They tend to have a significantly damaging effect on individuals and society at large and they impact on the systems and assets that facilitate the normal functioning of societies.

Risks in the ***social environment*** arise from a change in values, beliefs, human behavior and the condition of social structures. Tchankova (2002) suggests that changes in these variables could possibly result in strikes, riots or general social unrest, which could negatively impact the economy of a country and obstruct social development.

The ***political environment***, can cause risks due to a country's ruling party, which influences the way organizations conduct their business. This may be demonstrated by the reallocation of government funds from one industry sector to another or the changing of tax systems, which undermines the best interests of the shareholders (Tchankova, 2002).

The operational activities of an organization are a major source of risk which form part of the ***operational environment***. Workers may be at risk of personal injury should unfavorable working conditions result in some malfunction to an installation or production process. This will affect the personal, physical and mental well being of the employees and result in some financial expense to the organization resulting from such injuries on duty (IODs). It is equally feasible that the manufacturing processes of an organization could harm the natural surroundings making it important for companies to carefully plan and monitor their production and manufacturing strategies (Tchankova, 2002).

Sources of risk may arise in an ***economic environment***. The globaliza-

tion of markets and trading make its controlling such by a single government completely impossible. Global economic risks include economic recession and depression and at a localized level, can include interest rate or credit policy issues (Tchankova, 2002). These can have an impact on the gross imports and exports of a country and cause fluctuations in supply and demand thereby affecting company profit margins.

In addition to this, the ***legal environment*** has the potential to generate risks in business. Tchankova (2002) suggests the legal system generates risks through inconsistency between current and new legislation. The variation of legal standards from country to country has the potential to cause immense complexity and this can result in conflict between business partners (Tchankova, 2002).

Lastly, the ***cognitive environment*** is concerned with risks resulting from the differences in peoples perceptions and understanding of the world around them. Tchankova (2002) motivates that there are differences between perception and reality for various individuals and this is a significant source of organizational risk. These different perceptions raise questions regarding whether such perceptions of risk are valid and whether assessments regarding the effects of risk and uncertainty, which are based on these perceptions, produce factual results (Tchankova, 2002). This problem correlates with the different perceptions of risk in the various domains of scientific study and the different means of risk assessment, based on these perceptions.

The environments, which are sources of risk have now been identified and it is important to emphasize that the fundamental goal is to control risks. Therefore, it is essential to explore how risks should be addressed to control them to a level that is deemed acceptable.

2.2.4 Addressing Risk

Since ancient times people have sought ways of dealing with the numerous risks which have the potential to negatively impact upon individuals and society. As far back as 1700 BC the ancient Babylonians were aware of the potential financial risks involved in their international trade endeavors. These included anything with the potential to disrupt or prevent the safe passage of commodities between countries. Consequently, they sought to implement rudimentary countermeasures to sustain their international trade

relations (Valsamakis, Vivian, & du Toit, 1992). Additionally, around 700 BC the ancient Greeks and Phoenicians were beginning to employ similar means to deal with the trade risks they were encountering. The procedures they were employing apparently offered simple improvements over the initial attempts of the ancient Babylonians (Valsamakis et al., 1992). Furthermore, these procedures for dealing with risk were considered the first authentic means of mitigating the risks associated with international trade ventures and eventually led to the development of the current insurance industry. (Valsamakis et al., 1992).

The process of dealing with risk today has developed considerably since ancient times. Risks are now dealt with in a much more formal manner through highly specialized and structured processes constituting the broader concept of Risk Management. Risk Management plays an important role in addressing the various risks that have the potential to cause damage to people, their systems and other related assets. This is especially true in business where the implementation of a Risk Management plan will mean the difference between profitability or the survival of the organization. There is a need, therefore to scrutinize the process of Risk Management in more detail and explore what this process entails.

2.3 Risk Management

It is necessary to identify and manage all potentially harmful risks by some form of Risk Management activity for an organization to remain sustainable. Risk Management is a essential component of any organization's overall corporate responsibilities.

2.3.1 Risk Management Defined

There will always be some form of risk involved irrespective of what type of product or service an organization produces. Consequently, organizations should seek to manage those risks effectively by implementing a Risk Management framework and related system of internal control which addresses the pertinent aspects of enterprise risk. The Committee of Sponsoring Organizations of the Treadway Commission (COSO, 2004), developed an internal control framework, the "*Enterprise Risk Management - Integrated Framework*"

which has become the de facto standard for developing an enterprise-wide Risk Management solution (Preventsys, 2005). The COSO (2004) framework defines the overall process of Risk Management as:

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

The definition begins by stating that Risk Management is a process accomplished by the BoD, management and all other organizational personnel. The BoD is ultimately responsible for ensuring that their Risk Management practices are effective, however, the King Report (2001) states that it is the equal responsibility of management and staff to ensure that Risk Management strategies are properly implemented and executed. The King Report (2001) is a report on Corporate Governance compiled by the King Commission under the auspices of the Institute of Directors in South Africa and will be discussed in more detailed in subsequent sections. The above mentioned definition further states that "Risk Management is applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity". The King Report (2001) clarifies this in stating that:

> *Risk Management "refers to the total set of interventions in matters as diverse as a company's organizational design, culture, the ethical climate conveyed by the Board and senior management, recruitment criteria, key financial, operational and other processes and chosen indicators of good or desired performance."*

The process of Risk Management aims to address the following: all areas of risk, in every facet of the organization, through the development of sound Risk Management strategies that support the attainment of business goals. Finally, the definition concludes that Risk Management allows an organization to moderate its risks to within its risk appetite to ensure it is able to achieve its business objectives. This risk appetite can be described as the amount and type of risk the organization is prepared to accept, without such

risk having an effect on its ability to achieve its business goals and produce business value. Risk appetite is usually determined by establishing the financial viability of controlling a risk compared to the consequences of not controlling it. Each organization may differ on what their risk appetite is while in pursuit of growth and capitalizing on opportunities for the organization, its shareholders and stakeholders (King Report, 2001). The decision of the level of risk for any organization is subjective and unique.

The Risk Management practices of an organization need constant review and adjustment to remain effective and to continue to adequately serve its best interests. The King Report (2001) states that there should be a dedicated committee responsible for the constant review of Risk Management processes, in terms of their effectiveness, and risk profile. Additionally, Preventsys (2005) states that the process of organizational Risk Management itself should not be conducted as a single exercise but as an ongoing process of recognizing and reacting to potential risks. These reviews and adjustments refine these processes, ensuring they continuously add value to the organization by managing risks as effectively as possible. A central feature of Risk Management is repetition and review.

Preventsys (2005) has enumerated the following characteristics which are central to the overall Risk Management process:

- An ongoing cyclic process;
- Involvement of everyone in the organization for maximum effectiveness;
- Utilized in organizational strategy setting;
- Operates at every level of the enterprise, within every business unit and department;
- Aims to identify all pertinent aspects of organizational risk and manage these risks within the organization's risk appetite;
- Provides reassurance to management and the BoD that enterprise risks are being adequately addressed;
- Enables the organization to achieve its business goals and objectives with greater ease.

Risk Management is, thus, an important function in any organization because it helps to minimize risk and create business value by recognizing and reacting to potentially harmful risks through the planning, arranging and controlling of various activities and organizational resources (King Report, 2001). Such planning, arranging and controlling efforts would include a certain amount of funding, insurance and emergency planning (Simister, 2000). Risk Management will help to dissipate the criticality of organizational risks to a more acceptable level within the organizational risk appetite and aid the accomplishment of business objectives. The concept of Risk Management has developed over a long period of time. It is necessary to examine the origins of Risk Management to understand how it came to play such a major role in modern day organizations.

2.3.2 The Origins of Risk Management

According to Terry Simister, Chairman of the Institute of Risk Management (IRM), the idea of Risk Management was first presented in the United States of America as far back as the early 1950's and then later surfaced in the United Kingdom during 1969. Doug Barlow of Massey Ferguson gave the first formal presentation on the subject. Shortly hereafter, the Association of Insurance Managers in Industry and Commerce (AIMIC) incorporated an "R" into their title and became the Association of Insurance and Risk Managers in Industry and Commerce (AIRMIC). This change necessitated numerous insurance managers to identify themselves as "risk managers" and they began to practice Risk Management activities. Simister (2000) further illustrates that over the following couple of years the term Risk Management started gaining great popularity to become one of the latest buzzwords to be adopted by the insurance underwriting and broking disciplines. Individuals in these fields of expertise began consulting and providing advice and assistance on developing various Risk Management programs dealing with financial risks. The prominence of Risk Management became evident as many disciplines began to see the significance of developing their own Risk Management activities dealing with their field specific risks. Consequently, by 1985, Risk Management had grown to become an accepted and renowned field of expertise. During the next few years, numerous professional organizations were founded specializing in establishing Risk Management standards for the

development of skills in this field. The Institute of Risk Management (IRM) is one example and was established in 1986 (Simister, 2000).

The concept of Risk Management, today, is applied to more than financial risks. Various disciplines such as engineering for example have developed well established Risk Management methodologies which are specifically suited to dealing with numerous discipline-specific risks. These Risk Management practices employed in the various disciplines differ and each has their own way of Risk Management. However, despite the differing activities each discipline uses to deal with their own unique risks, they ultimately follow one of several generic Risk Management strategies. It is necessary to discuss these generic means of implementing Risk Management in more detail to gain a clearer understanding about how Risk Management is generally applied in business.

2.3.3 Various Strategies for Implementing Risk Management

Risk Management, today, is required to be a routine part of organizational daily business activities (Blakley, McDermott, & Geer, 2001), to enable the generation of business value and consequently serve shareholders interests. There are generally four basic approaches to managing the risks that businesses currently face. Whitman and Mattord (2003a) have more specifically defined these as strategies for risk control which include risk avoidance, risk transference, risk mitigation and risk acceptance.

Risk avoidance is a Risk Management strategy that focuses on evading risks instead of addressing the consequences of these risks should they occur (Whitman & Mattord, 2003a). Risk avoidance is an ideal option but not always practical. Blakley et al. (2001) discusses two general ways of avoiding or indemnifying oneself against risks namely, pooling and hedging.

- In a pooling scheme the cost of a particular risk is shared by several organizations. If the risk is not likely to occur simultaneously to the majority of the organizations in the pool then the cost of the risk to each of these organizations will be minimized. Insurance policies are said to be the most common types of risk-pooling schemes.

- In a hedging scheme an organization wagers it will experience the adverse effects of some risk, whereas other organizations may see this

as unlikely and accepts the wager. Furthermore, if the said risk does indeed result in some adverse event the bettors have to pay the organization, which has in a sense won the wager. Thus, the organization uses the money from winning the wager to settle the costs incurred due to the adverse event caused by the risk (Blakley et al., 2001). However, if the organization loses the wager it will have to pay off the bettors. One of the most common means of employing a hedging scheme is through options. McKoen and Gough (1997) suggest that options are very similar to insurance policies as an organization may purchase an option by paying premiums and consequently use the option only when necessary (McKoen & Gough, 1997).

A ***risk transference*** strategy aims to shift the responsibility for a certain risk onto another party (Whitman & Mattord, 2003a). An organization is able to transfer its responsibility for a particular risk by one of two means, by disclaimer or by agreement according to Blakley et al. (2001).

- When an organization decides to transfer their liability for a certain risk by disclaimer when they commence with a particular business activity, they must clearly state that they cannot be held responsible for the consequences of such an activity should a risk arise that results in an adverse event. Furthermore, the party who should be held responsible for the consequences of the risk is not clearly indicated.

- On the other hand, when an organization decides to transfer their liability for a certain risk by an agreement when they undertake a specific business activity, the party responsible for the consequences of the risk is specified (Blakley et al., 2001). This party is usually the party that the organization conducts the business activity for.

A ***risk mitigation*** strategy involves reducing risk to a more acceptable level by means of reducing either the probability of its occurrence or by reducing its consequences should it occur. The systems or processes possibly responsible for the generation of risks may require re-engineering to eradicate the known or suspected causes to reduce their probability of occurrence (Blakley et al., 2001). It may be necessary to reduce the consequences of a risk, once it has occurred and steps may be required to restrict the damage

(Blakley et al., 2001). Blakley et al. (2001) suggest that this can be achieved by either preventing such consequences from spreading or by decreasing the time it takes for the event to cause damage by decreasing discovery time and recovery time.

Finally, the last strategy involves ***risk acceptance*** where the organization retains responsibility for the consequences of risk. The organization attempts to absorb these consequences without implementing strategies for risk transfer, avoidance or reduction. A risk acceptance strategy may be implemented if the risks faced are of of negligible importance. This depends on the risk appetite of the organization is.

An organization may implement more than one of these Risk Management strategies. This is dependent on the types of risks that the organization may face. For instance, some risks may be unacceptable and the organization will choose to avoid them. Other risks, however, may also be significant but the benefits to be gained by taking on these risks may also be great and thus these types of risks may be mitigated to a more acceptable level. Additionally, other risks may be minor and are accepted as there is no significant impact on the business. An important point to consider is the identification and further analysis of which risks an organization may face for their appropriate management. The process of Risk Management is reliant on supporting activities which help to determine which risks an organization is susceptible to and how these risks need to be managed.

2.3.4 Risk Management Supportive Activities

Currently, one of the best known exercises used to identify and assess risks is Risk Analysis. IT is a process which includes the identification of threats most likely to significantly impact an organization and further scrutinizes the associated susceptibilities of an organization to these threats (Wold & Shriver, 1997). Frosdick (1997) motivates that Risk Analysis is a process comprising three consecutive phases. These include:

- Risk identification;
- Risk estimation;
- Risk evaluation.

These three phases produce useful information which provide Risk Management activities with appropriate guidance in terms of effective action to deal with risks. The process of Risk Analysis will be discussed in greater detail in subsequent chapters.

In this chapter the concept of risk has been examined highlighting its different perceptions among the various scientific domains. Furthermore, it was noted that, despite these various view points, the underlying perception common to all disciplines is that risk, in whatever form, needs to be controlled. Risk Management was identified and discussed in great detail as the most commonly applied activity by which risks are effectively addressed. The main function of Risk Management was described as managing and controlling various activities and resources to effectively manage risks. These activities form part of the responsibilities of the BoD (King Report, 2001). Risk Management plays an important role in ensuring the best interests of the shareholders are preserved. Risk Management is a component of a larger function that enables the BoD to ensure that the organization produces business value and preserves the interests of the shareholders. This broader function is known as Corporate Governance.

2.4 Corporate Governance

Corporate Governance is an important function in any organization with regards to preserving shareholder interests. It is the system that dictates how an organization is generally directed and controlled and includes the activities to direct and control Risk Management efforts. It will be examined in more detail to illustrate its importance to any organization.

2.4.1 The King Report on Corporate Governance

The King Report on Corporate Governance is a prominent source of information relating to the concept of Corporate Governance in South Africa. Its publication in November 1994 promoted the formalization of Corporate Governance as a fundamental function in business in South Africa (Thomson & von Solms, 2003). Its primary intention is to "promote the highest standards of Corporate Governance in South Africa" (King Report, 2001). The original King report, when published, was deemed internationally as the most

comprehensive publication on Corporate Governance (Institute of Directors of Southern Africa, 2002). The King Report has surpassed the financial and regulatory features of Corporate Governance by encouraging an all-inclusive approach to sound governance in the interests of diverse stakeholder groups whilst having consideration for the key principles of good financial, social, ethical and environmental conduct (King Report, 2001). The King II Report[1], however, published in 2002, includes several amendments addressing additional matters of importance, including information technology which was absent from the original report (King Report, 2001). However, despite their guiding principles stated concerning what constitutes good Corporate Governance, the King and King 2 Reports do not demand compliance. They serve merely as a code of good business practice (Thomson & von Solms, 2003).

The King Report offers extensive information on the concept of Corporate Governance and serves as a resource for explaining what Corporate Governance entails and means to an organization.

2.4.2 Corporate Governance Defined

Corporate Governance, according to Grant (2003) is generally concerned with aligning the interests of management and the shareholders. Sir Adrian Cadbury however, in Corporate Governance: A Framework for Implementation, offered a more specific definition which clarifies what Grant (2003) has stated. Sir Adrian Cadbury asserted that "Corporate Governance is concerned with holding the balance between economic and social goals and between individual and communal goals ... the aim is to align as nearly as possible the interests of individuals, corporations and society." (World Bank Group, 1999).

These definitions illustrate that organizations are involved in a balancing act as they continuously weigh the interests of their stakeholders against the demands of society. There are a wide variety of issues that organizations need to consider in order to operate effectively in the current dynamic business environment. The King Report (2001) clarifies this by stating that "boards have to consider not only the regulatory aspect, but also industry and market

[1]The King Report (2001) is the draft copy of the King Report which was published as the King II Report in 2002.

standards, industry reputation, the investigative media, and the attitudes of customers, suppliers, consumers, employees, investors, and communities (local, national, and international), ethical pressure groups, public opinion, public confidence and political opinion, etc."

Corporate Governance is ultimately about sound leadership efforts (King Report, 2001). Sound leadership and good Corporate Governance are exemplified by several characteristics which typically include accountability, responsibility, discipline, transparency, independence, fairness and social responsibility (King Report, 2001). These provide a good primer for implementing an effective approach to Corporate Governance in any organization and necessitate further discussion.

Accountability is ensuring that those who make decisions and act on them are answerable for these decisions and actions (King Report, 2001). In contrast, ***responsibility*** is ensuring that certain individuals are aware that they may be subject to disciplinary action following the negligence of their duties (King Report, 2001). ***Discipline*** involves requiring individuals to follow behavior generally accepted as being right and good (King Report, 2001). Additionally, ***transparency*** is concerned with demonstrating whether or not shareholders receive a realistic representation of activities taking place in an organization (King Report, 2001). ***Independence*** demonstrates the ability of the organization to mitigate or avoid possible conflicts of interest due to the authority of prominent executives or shareholders (King Report, 2001). Conversely, ***fairness*** is ensuring that the rights of all shareholders, large or small, are recognized and valued (King Report, 2001). The final characteristic, ***social responsibility*** involves demonstrating that an organization is concerned with environmental and human rights matters and is not discriminatory or exploitative (King Report, 2001).

The BoD must practice fairness, transparency, accountability and responsibility in every action taken and remain accountable to their organization but nonetheless act responsively and responsibly to the stakeholders (King Report, 2001). Good Corporate Governance is an important function in an organization and therefore the need for good governance should be addressed.

2.4.3 Addressing Good Corporate Governance

Ultimately the quality of organizational governance practices is the only means of assurance that shareholders possess ensuring they will receive good returns on their investments (King Report, 2001). Corporate Governance is important because it is the mechanism that ensures the best interests of the shareholders. Shareholder interests are best upheld through the proficient utilization of valuable and limited organizational resources and accountability for their management is a key characteristic of Corporate Governance (World Bank Group, 1999).

Today it is important that organizations do not fail to demonstrate both accountability and responsibility for the decisions and actions taken by their senior management and boards of directors. Organizations must realize that they should not attempt to function autonomously from the social orders or environments in which they exist (King Report, 2001). According to Thomson and von Solms (2003), organizations are a more direct presence to the general public than the government is. Organizations should, therefore, be compelled to demonstrate the characteristics that comprise a sound approach to Corporate Governance if they wish to gain trust and support from the communities and markets that they provide services to.

A survey carried out by McKinsey and Company, showed that investors who sought a strategy for growth were unconcerned about Corporate Governance, whereas investors who sought a value strategy and invested in undervalued or secure organizations were prepared to fund good Corporate Governance (Agrawal et al., 1996). It is apparent that investors may believe that an organization which demonstrates good Corporate Governance will operate better over a period of time and that good Corporate Governance will serve to reduce organizational risks and draw potential investment (Agrawal et al., 1996).

External scrutiny over company operations has intensified due to an apparent lack in the ability of Executive Management and corporate boards in providing effective direction and control over the affairs of their organizations. These organizations have failed to effectively express the characteristics of good Corporate Governance. Corporate Boards are now expected to comply with a myriad of new laws and regulatory compliance mandates or face the consequences. These may potentially involve strict financial penalties or

lengthy prison terms for responsible executives if convicted (Trillium Software, 2004). Regulatory intervention is not the preferred option, because this could result in the tarnishing of the corporate image and lead to the loss of consumer and investor trust (Vericept Corporation, 2004).

Some examples of the various regulatory and legislative requirements currently in effect include the Sarbanes-Oxely Act (SOX), The Gramm-Leach-Bliley Act (GLBA), The Health Insurance Portability and Accountability Act (HIPAA) and the international Basel Capital Accord (Basel II). There are more regulations, some of which general, while others are specific to a particular industry (Trillium Software, 2004). The regulations mentioned here, for example, have a significant global influence on data management activities (Trillium Software, 2004), emphasizing the importance of information privacy and promoting stronger internal control mechanisms (Vericept Corporation, 2004). Some of these regulations will be discussed in greater detail in subsequent chapters.

Generally, various legislative and regulatory requirements demonstrate that corporate executives and the BoD are both accountable and responsible for their decisions and actions. The placement of this accountability and responsibility requires a better managed corporate environment. There is a need to promote self governance, through an improved system of Corporate Governance, as an alternative to more legislation. The introduction of new legislation does not alleviate the current situation on its own (Entrust, 2004a).

Good Corporate Governance can be seen as a key to economic success and the stability of an organization by promoting sustained organizational growth through a value adding strategy that attracts investment. However, implementing a system of Corporate Governance is not without its challenges.

2.4.4 Corporate Governance Challenges

One of the most fundamental challenges organizations currently face in implementing the most effective approach to Corporate Governance is achieving a balance between company performance and conformance to any constraints placed on an organization (King Report, 2001). Organizations need to consider the expectations of their shareholders for acceptable financial growth as well as their responsibilities toward fulfilling their obligations to other or-

ganizational stakeholders (King Report, 2001). This entails complying with various laws and regulations and showing consideration for any social or ethical pressures that society may place on an organization. An organization must find acceptable means of generating shareholder value. The definition of Corporate Governance itself, as stated previously, suggests that a balance between performance and conformance is necessary for good governance. The intention of Corporate Governance is to seek an equilibrium between enterprise and accountability rather than place outright constraints on an organization (World Bank Group, 1999). However, as organizations endeavor to balance performance and conformance they should guard against falling into the three "corporate sins" as described by Tomorrow's Company in the United Kingdom. In this context these are sloth, greed and fear.

Sloth can be described as the loss of flair when an organization gives way to its administration (King Report, 2001). Business involves taking on a certain amount of risk and managing that risk, however, sloth is evident when an organization becomes lazy and attempts to circumvent even calculated risks (King Report, 2001).

Greed, in this context, is evident when corporate executives make short-term decisions seeking instant gratification in terms of personal financial gains relating to share options and other bonuses. Such decisions have no lasting benefits and do nothing to bolster long-term organizational prosperity (King Report, 2001). Such executives seek nothing more than personal enrichment.

The third corporate sin, ***fear*** manifests when corporate executives become submissive to the demands of investors and fail to acknowledge their own ambition for corporate sustainability and enterprise, because the investors may not share the same ambitions (King Report, 2001).

These three corporate sins have the ability to cripple an organization, making it unable to perform at maximum potential, generating substantial business value and fully preserving the shareholder interests. Some examples of corporate governance failures can be found in chapter 6 in section 6.2.2. The pro-active engagement of Executive Management and the BoD in demonstrating those characteristics that constitute good Corporate Governance, will result in a good balance between performance and conformance and the corporate sins can be avoided. This will ensure that an organization

performs at a satisfactory level for its relevant stakeholders. The existence of an organizational structure enables the organization to effectively demonstrate the characteristics of good governance, avoid the corporate sins and effectively guide its business to produce significant shareholder value. This organizational structure comprises the hierarchy of personnel and other relevant parties which influence the Corporate Governance function. It is necessary to discuss this organizational structure to demonstrate how Corporate Governance is approached within an organization.

2.4.5 Corporate Governance and Organizational Structure

The Board of Directors

An organization is presided over by the BoD, a group of persons elected by the shareholders of the organization to represent their interests through the proper governance of the organization (BambooWeb Dictionary Open Content Encyclopedia, 2005a). The BoD comprises the chairperson, the Chief Executive Officer (CEO) and various executive and non-executive directors (Thomson & von Solms, 2003). The establishment of organizational vision, principles and the strategy that realizes the vision is a key responsibility of the BoD (King Report, 2001). The BoD's fundamental obligation is to demonstrate their fiduciary duty towards upholding the best interests of the organization and stakeholders (TIAA-CREF, 1998). The BambooWeb Dictionary Open Content Encyclopedia (2005d) describes fiduciary duty as being grouped into three broad categories, namely, duty of loyalty, duty of candor and the duty of care.

- ***Duty of loyalty*** is achieved by acting in accordance with a beneficiaries best interests and not their own;
- ***Duty of candor*** is achieved by being open and transparent in terms of the disclosure of information to a beneficiary, specifically with regard to transactions between the fiduciary and the beneficiary;
- ***Duty of care*** is achieved by demonstrating prudence with regard to the interests of the beneficiaries.

The BoD exercises their fiduciary duty by defining various processes and procedures aiming to protect organizational assets and corporate reputation (King Report, 2001). These include efforts to ensure the organization complies with any regulatory and legislative mandates and other codes of good business practice appropriate to the organization (King Report, 2001). Additionally, the BoD is required to recognize significant aspects of organizational risk and key performance indicators to enhance shareholder value by generating acceptable profits (King Report, 2001).

Board Committees

Board committees, according to the King Report (2001), facilitate the BoD in fulfilling their responsibilities sufficiently and appropriately. Board committees are more focused and dedicated to dealing with specific issues in greater detail. Therefore, board committees are able to ensure that particular issues receive enough consideration enabling the full BoD to reach impartial and unbiased decisions (King Report, 2001). Board committees facilitate the BoD significantly in addressing the interests of the shareholders.

There are a variety of board committees. Some are standing committees which perform ongoing functions on behalf of the BoD (King Report, 2001). The Risk Management committee is an example of a standing board committee. It assists the BoD in corporate accountability and any risks related to management, assurance and reporting (King Report, 2001). Its terms of reference include disaster recovery risk, technology risk, operational risk, and compliance and control risks (King Report, 2001). There are also temporary board committees, which are assigned unique once-off tasks and are disbanded upon their completion (King Report, 2001).

The Chairperson

The BambooWeb Dictionary Open Content Encyclopedia (2005b) states that a chairperson "is the presiding officer of a meeting, organization, committee, or other deliberative body". It is the responsibility of the chair to provide the BoD with sound leadership guaranteeing the smooth functioning of the BoD to promote good governance. The chair must ensure that the BoD receives adequate information enabling them to make informed decisions (King Report, 2001). The chair must ensure that good relations are

maintained between the organization and its shareholders and act as the primary link between the BoD and management, and between the BoD and the organization's CEO (King Report, 2001). The chair may be given various other executive powers to achieve these relationships (BambooWeb Dictionary Open Content Encyclopedia, 2005b).

The Chief Executive Officer

The Chief Executive Officer (CEO) is the top ranking executive in terms of the management of organizational daily operations and has executive authority within an organization (BambooWeb Dictionary Open Content Encyclopedia, 2005c). The CEO is the primary organizational representative, acting as chief spokesperson and key role-player in the implemention of organizational strategy to achieve operational business success (King Report, 2001). The CEO is required to develop and propose the high-level strategy and vision that will best benefit the organization to produce significant shareholder returns and nurture good relations with other appropriate stakeholders (King Report, 2001). Furthermore, the CEO must ensure the daily business operations are suitably monitored and managed. He/She must plan and supervise the implementation of significant corporate policies (King Report, 2001). The CEO is commonly a member of the BoD and reports back to the BoD on the operational affairs of the organization. It is not uncommon for the CEO to act as Board Chairman, however, these positions are often kept separate to avoid an imbalance of power and the domination of a particular individual which helps to thwart conflicts of shareholder interests (BambooWeb Dictionary Open Content Encyclopedia, 2005c).

The Shareholders

A shareholder can any entity i.e. an organization or person that legally holds possession of one or more shares of stock in an organization. Shareholders may hold special rights depending on the type of stock they own. For instance such rights may include:

- The right to vote on who may represent their interests on the BoD;
- The right to claim a portion of the organization's profits;

- The right to buy more shares in the organization if they so wish;
- The right to claim various organizational assets should the organization fall into liquidation (BambooWeb Dictionary Open Content Encyclopedia, 2005e).

There are essentially three types of shareholders, shareowners, contractual shareholders and non-contractual shareholders.

- Shareowners include those parties who legitimately own stock, through mutual funds (New York Stock Exchange, 2001);
- Contractual shareholders include those individuals that have a relationship with an organization based on some contract or agreement, for example the personnel, suppliers and customers (Thomson & von Solms, 2003);
- Non-contractual shareholders are those parties having a relationship with the organization which is not based on some contract or agreement. Typical examples of non-contractual shareholders include the government and other authorities (Thomson & von Solms, 2003).

It is important to emphasize that there should exist a clear and constant channel of communication between the BoD and the shareholders in the interests of good Corporate Governance (Thomson & von Solms, 2003). The BoD is responsible for presenting the shareholders with a detailed organizational performance report which should include both successes and failures (BDO, 1999).

The unified and harmonious functioning of these concerned parties can create an effective approach to Corporate Governance that strikes a balance between organizational performance and conformance. Corporate Governance serves as the mechanism that ensures the best interests of the shareholders are upheld. However, a fundamental aspect of satisfying shareholder expectations involves risk control as part of the broader Corporate Governance function. The King Report (2001) states that "enterprise is the undertaking of risk and reward" and Risk Management features strongly in Corporate Governance because it controls enterprise risks and increases organizational and shareholder returns. An organization must understand its

risks while fulfilling its business objectives and the various strategies implemented to address risks for the BoD and stakeholders to understand organizational affairs (King Report, 2001). For this reason, the controlling of risks plays an important role in implementing Corporate Governance and preserving shareholder interests, therefore, it is necessary to explore the relationship between Corporate Governance and Risk Management. It is also necessary to highlight the BoD's Risk Management responsibilities which form a component of the Corporate Governance function.

2.5 Risk Management and Corporate Governance

The process of preserving shareholder interests would be ineffective where Risk Management does not form a fundamental component of Corporate Governance. It is necessary to clarify this point by exploring why and what can be done to ensure that Risk Management is adequately integrated into the Corporate Governance function.

2.5.1 The Importance of Risk Management as a Corporate Governance Responsibility

The ultimate responsibility of the BoD, as previously stated, is to provide strategic direction to an organization and remain in complete and successful control over its affairs (King Report, 2001). Such efforts include ensuring the organization continues to comply with any applicable laws and regulations (King Report, 2001). It it is important for the BoD to address all pertinent aspects of enterprise risk to fulfill their regulatory obligations. Borland Software Corporation (2005) suggests that a general failure to appropriately manage risk can lead to professional and personal loss. These could typically include high customer turnovers, loss of business associates, stringent legal intervention, overlooked market and revenue opportunities and the total loss of business operations (Borland Software Corporation, 2005). These events are risks that every organization should seeks to avoid as they endeavor to generate profits, attain competitive advantage and sustained corporate development. All businesses do face risks, but if these are understood and

appropriately managed, taking the right risks can produce competitive advantage (Borland Software Corporation, 2005).

Risk Management can be seen as a business enabler allowing an organization to become aware of various issues not necessarily previously considered. Risk Management helps to avoid unexpected events by making certain that appropriate insights have become evident further aiding the decision making process and enabling the creation of countermeasures and controls before the risks become a real hazard (Borland Software Corporation, 2005). Borland Software Corporation (2005) suggests that Risk Management enables an organization to "gain a strategic discipline for operational excellence, as well as the power to create and influence its desired future".

There is a commitment required from those at the head of the organization, namely the BoD, to endorse and implement Risk Management effectively as a Corporate Governance responsibility. The BoD is required to understand their corporate Risk Management responsibilities to ensure that Risk Management is effective.

2.5.2 Risk Management Responsibilities of the Board

The King Report (2001) on Corporate Governance provides comprehensive guidance on the responsibilities of the BoD about Risk Management. The BoD is the supreme authority in an organization and they must understand where all organizational risks lie to make well-informed decisions regarding organizational future. The BoD is, therefore, responsible for the complete Risk Management function which attempts to address all facets of organizational risk (King Report, 2001). The King Report (2001) recommends several fundamental activities that the BoD should execute to facilitate itself in achieving this objective, through a comprehensive Risk Management program. These activities include ensuring that all business functions commence in an acceptable manner providing protection for all organizational assets; maintaining compliance with various laws and regulations; guaranteeing there are measures in place to promote accurate risk reporting and remain confident that their organization is resilient to significant risks (King Report, 2001).

It is important to emphasize that the BoD must ensure that all the organizational Risk Management activities are executed regularly (King Report,

2001). This establishes that all risks, including new ones, have been successfully controlled. The successful management of these risks is an important concern for the BoD and entails their deciding on a suitable organizational risk strategy (King Report, 2001). These strategies were previously discussed and identified as risk acceptance, risk avoidance, risk transference and risk mitigation.

The Risk Management strategy chosen by the BoD must to satisfy the organizational risk appetite which is their responsibility to establish (King Report, 2001). Once a decision has been reached regarding the organizational risk appetite and suitable Risk Management strategy, the BoD must ensure the policies and procedures created complement the chosen Risk Management strategy. These should be disseminated to all personnel (King Report, 2001).

The implementation of the Risk Management policies and procedures must be constantly monitored by the BoD ensuring they are relevant in terms of managing existing risks and exposure to new risks (King Report, 2001). It is necessary for the BoD to receive regular Risk Management reports which highlight its effectiveness (King Report, 2001). This effectiveness can be gauged by conducting an annual Risk Analysis exercise.The conducting of regular Risk Analysis activities allows an organization to coordinate its Risk Management activities and maintain them to the current risk profile.

2.6 Conclusion

The implementation of Risk Management at a Corporate Governance level can have a dramatic and positive effect on an organization because these efforts will help the BoD to guide the business of their company successfully and avoid incidents that diminish business value and undermine shareholder expectations. The implementation of various Risk Management activities will demonstrate the characteristics of good Corporate Governance. It will help to balance organizational performance and conformance by allowing an organization to take both calculated risks and avoid harmful ones. This will create a trusting relationship between an organization, its shareholders and other stakeholders. The BoD must be vigilant in their Risk Management endeavors to achieve this.

The King Report (2001) illustrates the numerous Risk Management re-

sponsibilities of the BoD. These responsibilities necessitate communication and information on various aspects of organizational risk. The BoD require a holistic picture of the organizational risk profile to execute its Risk Management practices effectively. They require comprehensive reports various aspects of risk to enable them to prioritize the risk profile.

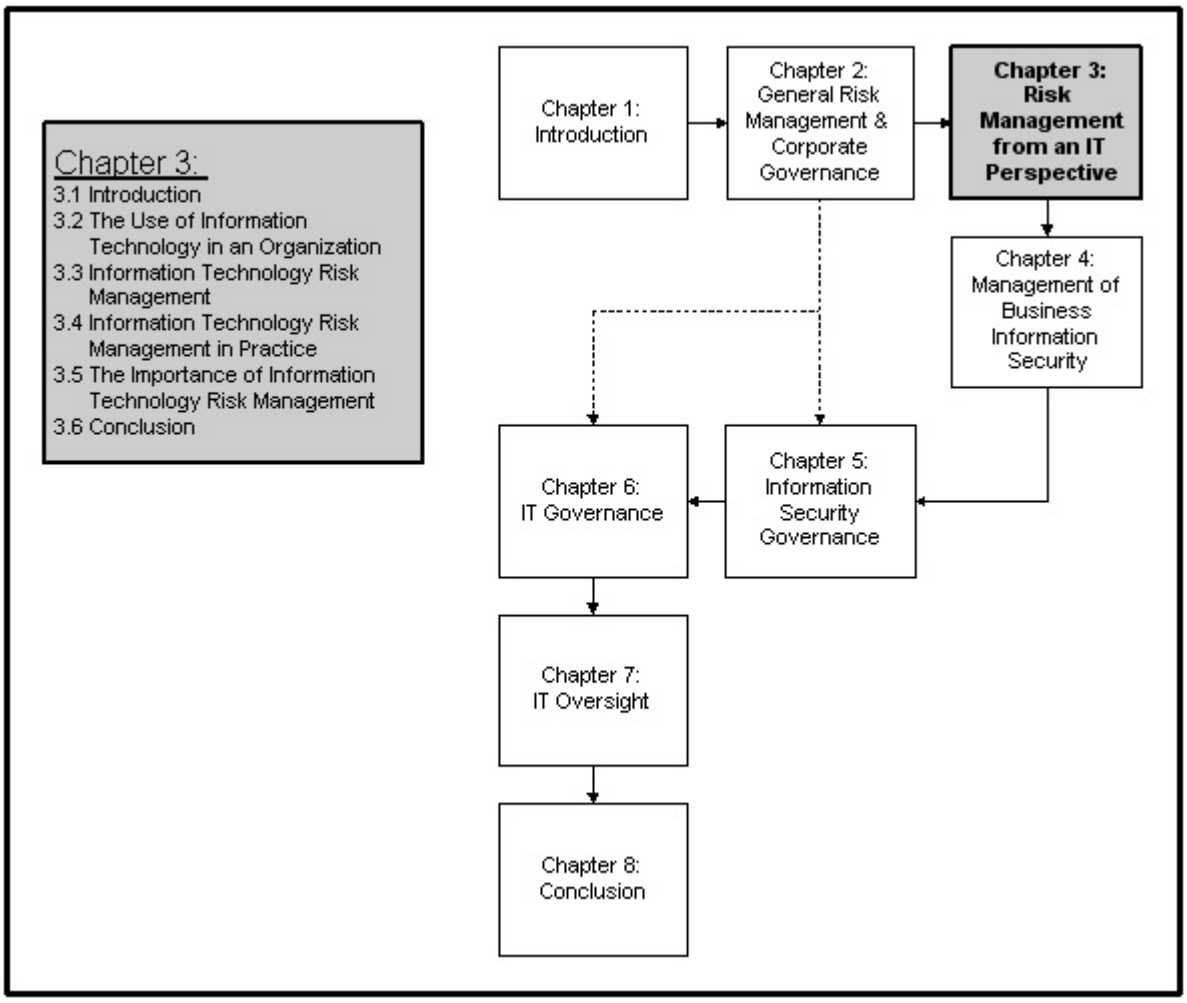
The vast integration of IT systems into most organizations requires consideration because Information Technology (IT) is a significant business enabler and an important means of managing valuable information assets and executing business operations. Any risks resulting from the reliance on IT can have a significantly negative impact on organizational business value if underestimated or undetected (Blakley et al., 2001). The identification and management of IT-related risks by an IT Risk Management activity is, therefore, very important and it plays an important role in aiding the BoD in fully addressing all key aspects of organizational risk. The concept of IT Risk Management will now be examined in more detail.

Chapter 3

Risk Management from an Information Technology Perspective

3.1 Introduction

There is a fundamental need to consider the risks associated with IT while its utilization aims to produce business value and ultimately satisfy shareholder expectations. These risks have the potential to greatly reduce business value and undermine the expectations of shareholders. It is important that organizations implement some type of IT Risk Management strategy to address such IT-related risks. Consequently this chapter aims to highlight the importance of IT Risk Management as a fundamental component of the broader Risk Management framework and Corporate Governance function. The influence of IT has had on most modern organizations is examined and its importance in enabling them to attain their business objectives is further discussed and the risks associated with IT's use. These risks demonstrate the need for IT Risk Analysis and Risk Management will be discussed in detail in terms their implementation relating to IT-related risks. The importance of IT Risk Management to allow such organizations to continue to function whilst achieving their business objectives seamlessly and still protecting company assets and upholding shareholder interests will be discussed.



3.2 The Use of Information Technology in an Organization

Information Technology has assumed an important role in most organizations today. The value that IT may produce requires discussion and it is important to highlight the risks associated with its organization-wide use and demonstrate the need to address such risks.

3.2.1 The Growth in Dependence on Information Technology

A clearer understanding of the importance of managing the risks associated with IT currently is gained through examining the role which IT plays in most modern day organizations. Over the past few decades there have been

major advances in technology and as a result organizations have sought to implement this technology to add business value by re-engineering business processes so they may provide more efficient services to customers and other stakeholders.

The development and subsequent implementation of IT as a service enabler and business value creator can be generally divided into three broad eras. During the first era computers had limited capabilities and were considered as dumb terminals. These computers were connected to large mainframe computers which were used to process the data of various organizational departments. Data was processed in batch mode by programs represented as decks of punched cards put through a card reader (Schneider & Perry, 2001). These mainframes were located in a centralized facility or computer department where data was processed (Gerber & von Solms, 2001). Access to this facility was restricted to those who were responsible for operating the mainframes and processing the batch jobs.

New technologies emerged and ushered in the second era in the history of computing. There were advances such as multiprocessing and high-speed communications. Smaller personal computers had come into use and were capable of performing a variety of functions and were more affordable (Schneider & Perry, 2001). Companies began to employ these computers to create their own internal networks (Schneider & Perry, 2001). Distributed computing became a reality as hardware and software resources were made accessible to computer users in remote locations enableding them to log onto disparate sites and work with programs and files located there (Flynn & McIver McHoes, 1997). Innovations such as email allowed company employees to communicate conveniently. Furthermore, organizations required external communication and larger organizations started building their own company-wide networks which utilized leased telephone lines enabling them to connect to various branches and company headquarters (Schneider & Perry, 2001). It was during this time that other organizational departments started becoming dependent on the continued functioning of what became known as the "Information Technology" department (Moses, 1992). It was their responsibility to automate the various business processes the other departments.

Later still, during the third era and currently, IT has begun to facilitate business processes and services to customers, business partners and other

stakeholders. IT had become a fundamental organizational asset and the services provided by an organization's information technology department had become of critical importance. Innovations such as the Internet began to enable many organizations to perform business transactions with their customers and other organizations with greater ease through electronic commerce. IT has become a major strategic enabler and has allowed companies to attain competitive advantage over one another (O'Brien, 2000).

IT has had a significant impact on the way organizations currently conduct their business functions. These organizations have realized there is much value to be gained from effectively implementing IT. Therefore, it is necessary to discuss the value of IT and demonstrate its importance and utility within most organizations today.

3.2.2 The Importance of Information Technology

Keen (1991) states that "information technology is reshaping the basics of business. Customer service, operations, product and marketing strategies, and distribution are heavily, or sometimes even entirely, dependent on IT. Information technology, and its expense, have become an everyday part of business". IT is a valuable organizational resource and its application can generate significant business value. IT has the ability to enhance the efficiency and effectiveness of business functions including the decision making abilities of executives. It can reinforce organizational competitive stance in the fast paced and dynamic markets of the modern world (O'Brien, 2000). Furthermore on an international scale, Internet-based technologies are rapidly becoming a fundamental constituent for success in business today (O'Brien, 2000). O'Brien (2000) suggests that IT and information systems have three important organizational roles:

- Facilitating the execution of organizational business processes and operations;
- Facilitating executives and other employees in their everyday decision making processes;
- Facilitating the strategies that allow an organization to attain competitive advantage.

Innovations, such as electronic commerce, have replaced the traditional means of commerce and allow organizations to increase profits and sales and reduce any resultant costs (Schneider & Perry, 2001). Electronic commerce assists in advertising and extending organizational reach to smaller geographically dispersed market segments (Schneider & Perry, 2001). Electronic commerce is able to provide consumers with a wider variety of purchasing opportunities and has increased the rate and precision with which organizations are able to exchange information (Schneider & Perry, 2001). It is but one manner in which IT can be applied to benefit an organization. In a more holistic sense, utilizing IT generally enables organizations to create products, services, processes, and capabilities that provide them with a strategic edge beyond that of competitors (O'Brien, 2000). There are, according to O'Brien (2000), three fundamental strategies that IT follows to create competitive advantage, cost strategies, differentiation strategies and innovation strategies (O'Brien, 2000).

- An ***cost strategy*** helps an organization to become an inexpensive manufacturer, reduce customer and/or supplier costs or increase competitors costs making it difficult for them to gain a secure position a particular field of business. Developing electronic commerce based web sites on the Internet to lower the costs of marketing is an example of an IT cost strategy (O'Brien, 2000).

- An IT ***differentiation strategy*** involves devising ways to utilize IT to set an organization's products or services apart from competitors so customers may observe these products or services as being more distinctive and attractive. An example of an IT differentiation strategy includes prompt and efficient customer assistance through the use of an Internet web site (O'Brien, 2000).

- An IT ***innovation strategy*** may involve launching brand new products or services that embrace elements of IT, or strategically applying IT to drastically revamp certain business processes that would have a major impact on the way business is carried out in the industry as a whole for example (O'Brien, 2000).

The current application of IT in business can provide an organization with the means to provide better services to customers and enable more efficient

dealings with suppliers and other business partners. IT can be classified as a useful tool in profit generation substantial and demonstrates a contribution toward increasing business value and shareholder returns. However, as organizations start to invest in IT to support their business goals they need to be aware of the risks associated with the implementation of IT.

3.2.3 The Risks Associated with Information Technology

It is necessary to explain how risk in the IT sense is perceived before embarking on an in-depth discussion about the various risks that affect IT. Blakley et al. (2001) describes risk as being the possibility of an incident occurring when its occurrence would have a negative impact on business value. Risk, in the IT sense, is viewed from a negative perspective and as having some detrimental impact on an organization. Risk from an IT perspective is said to be composed of three fundamental characteristics, assets, threats and vulnerabilities (Gerber & von Solms, 2001). IT risk is understood to mean the possibility of a threat impacting on an asset through some vulnerability.

An ***asset*** is defined as anything that an organization considers valuable which enables it to sustain itself as a competitive force in industry and produces business value. Assets are tangible or intangible. Tangible assets are those assets whose value can be accurately calculated. This includes physical objects like computers for example. Intangible assets are those assets whose value cannot be specifically gauged and whose value is not readily evident, although these assets are considered important. Examples of intangible assets include things like the business processes or the information resources and business data and organization uses uses to gain a better understanding of its customers needs and refine its strategy or business processes to cater for those needs.

Threats are those things that have the ability to damage or destroy the value of organizational assets. Potential threats to the IT assets are numerous and originate from several distinct categories including natural, technical and human threats (Wold & Shriver, 1997). Natural threats, which are referred to as acts of God, typically include floods, earthquakes, lightening storms, fires or even tsunamis for example. Technical threats refer to events such as

computer hardware or software failures and even power outages. Moreover, the threats that occur most frequently and are the most damaging result from the accidental or deliberate acts of human beings. They include intentional virus attacks on computer systems, the gaining of unauthorized access to confidential information i.e. hacking, or the destruction or modification of sensitive company data by unwitting employees or malicious individuals.

A ***vulnerability*** is a weakness or loophole left in the security of a system that a threat may exploit to gain access to and damage or destroy an asset, thereby reducing its organizational value. Programmers may create what a so-called a back door in the programs or applications they develop for example. This is typical of some operating systems, so that they can return and perform routine maintenance or other administrative functions. However, its presence can be viewed as a potential vulnerability because it represents an opportunity for a knowledgeable individual with malicious intent, to cause significant damage.

The risks associated with IT are not always significant or result in devastating outcomes, but to disregard them without appropriately considering their consequences would appear irrational. Bandyopadhyay, Mykytyn, and Mykytyn (1999) states that as IT spending increases and organizations become more technology dependent, they are increasingly susceptible to IT-related risks. It is necessary for organizations to ensure their assets remain secure from the consequences of potential risks as they employ IT to facilitate their daily business processes. They must implement security controls guaranteeing the safety of their business assets from significant risks to accomplish this. It is a necessity for these organizations to identify and control IT-related risks through IT Risk Management activities.

3.3 Information Technology Risk Management

Information Technology Risk Management should be a fundamental aspect of organizational business functions because they rely on IT to automate various business processes and support its services to customers and company stakeholders. IT Risk Management requires examination to define what it aims to accomplish and how its implementation will control the risks associated with technology dependence.

3.3.1 What is Risk Management in terms of Information Technology?

Risk Management, from the IT view point, can be defined as a process that enables equilibrium between the operational and economic costs associated with protecting organizational assets from IT risks, while attempting to achieve business goals (National Institute of Standards and Technology, 2001). IT Risk Management focuses on the selection and implementation of various appropriate security controls to effectively manage organizational IT-related risks. Humphreys, Moses, and Plate (1998) suggest that the cost of specific types of security controls is related to their implementation. This is because it is not economically viable to apply controls if their cost exceeds the value of the assets they protect or the budget that has allocated for security (Humphreys et al., 1998). It is important to consider that the budget for security is not too meager because this could affect the competence of organizationals Risk Management endeavors and result in unnecessary risks (Humphreys et al., 1998). The majority of organizations unfortunately have limited resources allocated to IT security (National Institute of Standards and Technology, 2001). It is important to correctly determine the security capabilities that IT systems require for risks to be appropriately controlled (National Institute of Standards and Technology, 2001). Using a good Risk Management methodology helps accomplish this and enables the selection of appropriate security controls needed to fulfill the security capabilities of organizational IT systems (National Institute of Standards and Technology, 2001). Humphreys et al. (1998) have enumerated various factors that should be considered when selecting appropriate security controls to manage IT-related risks. These include:

- How easy the control is to use?
- How transparent is the control to the user?
- Does the control help the user to satisfactorily accomplish their tasks?
- How effective is the control?
- What type of functions does the control support i.e. detection, prevention, recovery, deterrence, correction, monitoring or awareness?

A particular security control addresses several functions and preferably more than less. It is important to balance the types of functions that selected controls demonstrate to reinforce their overall ability to manage risks effectively and efficiently (Humphreys et al., 1998). A certain amount of residual risk will always remain after a selection of security controls have been implemented so an organization can never completely guarantee that its IT systems are completely secure (Humphreys et al., 1998). It would erroneous to assume that organizational assets are totally safe. IT Risk Management does reduce the impact of risks and provides management with a solid basis for accurate decision making to protect organizations against IT-related risks (National Institute of Standards and Technology, 2001). There are four general strategies through which an organization implements IT Risk Management. The type of strategy chosen depends on a number of factors. To gain a better understanding about which strategy best suits an organization they must be discussed in more detail.

3.3.2 Information Technology Risk Management Strategies

It is important that an organization adopts the appropriate strategy for the cost effective implementation of IT Risk Management. There are several factors that help an organization select a suitable IT Risk Management strategy based on its business needs which involves establishing its business environment and its business requirements for security. These security requirements typically depend on the following factors:

- Organizational size;
- The type of business the organization conducts;
- The organization's corporate culture (ISO/IEC TR 13335-3, 1998).

The level of detail at which IT-related risks are assessed and managed may vary in the application of various IT Risk Management strategies. This is because it would not be practical for smaller sized companies to conduct a highly detailed and thorough investigation of risks due to its being both resource intensive and time consuming. In contrast however, larger organizations would not benefit from a general high-level approach to IT Risk

Management because of their complex IT infrastructure and more detailed business security requirements. Organizations should attempt to identify a suitable approach to IT Risk Management or else they may experience some loss should the chosen strategy not fully support their business needs. It was mentioned in the previous section that there are essentially four general approaches to IT Risk Management. These include:

- The Baseline Approach;
- The Informal Approach;
- The Detailed Approach;
- The Combined Approach which comprises both the baseline and detailed approach.

The Baseline Approach

The Baseline Approach to IT Risk Management provides an organization with the means to manage IT risks at a basic yet adequate level. This level of Risk Management is commonly achieved by selecting a variety of security controls which can be appropriately applied to the critical information systems (Cho & Ciechanowicz, 2001). The implemented controls are normally suggested from baseline control manuals or codes of practice. An organization, using these manuals and codes of practice, is able to determine its fundamental security concerns and implement the controls required to address its most pertinent IT-related risks. Furthermore, these manuals and codes of practice attempt to motivate organizations to follow generally accepted security standards by suggesting the most effective means of addressing their basic security requirements. Both ISO/IEC TR 13335 (GMITS) and ISO/IEC 19977 are internationally accepted security standards providing comprehensive guidance in terms of implementing security which satisfies the organizational requirements for baseline security. The Baseline Approach to IT Risk Management has several advantages. Not much expertise are required to implement this strategy, it is not resource intensive and he identification and implementation of security controls involves minimal costs and time.

Cho and Ciechanowicz (2001) suggests that security control checklists may be utilized to provide guidance on the implementation of a baseline strategy because they help deliver a broad outline of the basic organizational security needs. It is important to consider all aspects when implementing a baseline strategy.

ISO/IEC TR 13335-3 (1998) states it is important to consider the granularity of the Baseline Approach. If the granularity is too coarse this could result in insufficient security controls that will not satisfy the organizational needs for IT security. If the granularity is too fine this may incur unnecessary costs due to the implementation of unnecessary controls. Additionally, if the granularity is too fine this could result in the implementation of excessively strict security measures. This proves to be frustrating to users who will find it difficult to carry out their daily business activities with some degree of convenience. An additional concern regarding the baseline approach involves the management of changes to security because system upgrades make it difficult to assess the effectiveness of currently implemented baseline controls (ISO/IEC TR 13335-3, 1998).

The Informal Approach

The Informal Approach to IT Risk Management is aptly named. It is not conducted in any structured manner. This is merely a quick and straightforward approach that addresses IT-related risks in a practical and rational way. The Informal Approach is conducted more rapidly than the detailed approach, which will be discussed next. The Informal Approach can be considered less resource intensive because it is both time and cost effective. This strategy is well suited for small to medium sized enterprises (SME's). It does not require the attainment of additional skills to implement the approach because it relies on the knowledge and experience of well-established personnel for its success (ISO/IEC TR 13335-3, 1998). These personnel are able to analyze the IT security requirements and suggest recommended safeguards to effectively control IT-related risks. This can be accomplished by brainstorming ideas regarding organizational IT-related risks based on their extensive knowledge gained through years of experience. However, when an organization lacks necessary expert skills an external consultant may be outsourced to provide insights into which controls would best manage IT-related risks.

A particular disadvantage of the Informal Approach however, is that some potentially harmful risks may be overlooked (ISO/IEC TR 13335-3, 1998). This may be because those conducting the exercise may unintentionally allow risks to go undetected or underestimated because of their subjective beliefs and opinions. Another disadvantage is that it is difficult to substantiate the costs of security controls selected for implementation because there is no solid basis upon which they were chosen except for an expert's subjective opinion. Lastly, the Informal Approach requires an organization to conduct continuous reviews to facilitate the management of changes to the security infrastructure (ISO/IEC TR 13335-3, 1998).

The Detailed Approach

The Detailed Approach to IT Risk Management is a more structured and methodical strategy. Risks are managed in a more formal manner. Typically, the Detailed Approach relies on IT Risk Analysis to provide information about risks and their effective control. It begins with the identification of important IT-related assets and any potential threats to determine which IT risks an organization needs to consider. Subsequently, the severity and possible frequency of each threat is considered based on organizational vulnerabilities which these particular threats can exploit. This enables an organization to determine the potential each risk has to negatively impact upon its business functions. Once the potential risks have been identified and evaluated, the next step is to organize these risks in some order of criticality. This is usually accomplished by employing a risk matrix. Risk matrices will be discussed later in this chapter. Once risks are organized according to criticality the organization will understand what their IT security needs are. The organization can then identify and implement security controls to manage its IT-related risks. A particular drawback of the detailed approach, however, is that it proves to be considerably resource intensive and requires constant attention from management (Humphreys et al., 1998).

The detailed approach has several advantages. It helps to establish a distinct representation of IT-related risks faced by an organization helps define organizational IT security requirements (Humphreys et al., 1998). Additionally, the information accumulated during its implementation assists with the management of security changes as systems upgrades occur (ISO/IEC TR

13335-3, 1998).

The Combined Approach

The final IT Risk Management strategy is the Combined Approach. It starts with the identification of the assets that are critical to daily business operations by a process of risk assessment based on the Baseline Approach (Humphreys et al., 1998). This assessment is used to separate the assets into distinct groups i.e. those requiring closer scrutiny of the risks affecting them (by implementing a more detailed Risk Management approach) and those for which a basic level of security is sufficient, and thus the controls selected for this group through the baseline approach are sufficient (Humphreys et al., 1998).

The Combined Approach to IT Risk Management has the advantages of both the Baseline Approach and the Detailed Approach (Humphreys et al., 1998). The Combined Approach is less time consuming whilst identifying the necessary security controls to ensure that an adequate level of protection is maintained. This is because less time is spent addressing the security requirements of assets that are less vulnerable to risks. An advantage of the Combined Approach is that limited organizational resources can be focused on prominent areas of risk and less resources are used on those risks with negligible consequences. It is however, important to correctly identify these differing areas of organizational IT risk. Failure to correctly establish this may cause certain aspects of an organization to be unnecessarily exposed to various potential IT risks leading to avoidable losses due to poor security design and implementation. The Combined Approach is considered the most cost effective and highly recommended strategy to implement to deal with the IT-related risks of an organization ISO/IEC TR 13335-3 (1998).

Each of these four strategies for IT Risk Management have their advantages and disadvantages. It is an organizational decision regarding which approach would best suit their IT security needs. Ultimately all these approaches result in the identification and subsequent implementation of an assortment of security controls that aim to reduce IT risk susceptibility. It is important to consider that security controls are selected based on the criticality of each risk and to establish their priority they need to be analyzed thoroughly.

Risk Analysis helps inform the process of Risk Management about which risks are most critical to ensure they receive an appropriate level of attention (Frosdick, 1997). Risk Analysis plays an important role in enabling the effectiveness of Risk Management. This is evident when considering the detailed approach to IT Risk Management. IT Risk Analysis will be discussed in more detail to understand its supporting role in effective IT Risk Management.

3.3.3 Information Technology Risk Management Supportive Activities: Risk Analysis

Risk Analysis is a well-known exercise used to identify and assess risks. It can further be defined as a process that involves identifying the threats, which are most likely to have a significantly negative impact on an organization, as well as scrutinizing the associated vulnerabilities to those threats (Wold & Shriver, 1997). It was previously stated that there are three processes that constitute a Risk Analysis exercise (Frosdick, 1997). These include:

- Risk identification;
- Risk estimation or assessment;
- Risk evaluation.

Each of these processes contribute toward producing meaningful information about organizational IT risks which helps to support IT Risk Management in selecting and implementing appropriate security controls.

Risk Identification

It is important to first identify what assets an organization needs to protect to successfully identify what risks they need to consider. In section 3.2.3 it was stated that assets can either be tangible, like physical computer hardware or networking equipment, or intangible, like the business processes that an organization relies on to help satisfy customer demands and produce business value. It is then important to identify the threats that may potentially impact on those assets. These may include any natural, technical and human threats. After assets and threats have been identified it is then possible to begin identifying all risks.

Risk identification is concerned with revealing all possible hazards that an organization may face, as a product of its assets and the threats which place those assets in danger, by the utilizing various risk identification techniques. Frosdick (1997) mentions one technique which entails a group of analysts sharing ideas with respect to what incidents may negatively impact on an organization. This method is applied in an attempt to speculate which risks need to be addressed to provide assurance regarding the safety of organizational assets. Another risk identification technique involves the utilization of security control checklists, as previously mentioned. These checklists extensively list every possible security control that could be implemented (Baskerville, 1993). Checklists enable an analyst to select suitable security controls on the basis of the asset and threat identification and the existence of implemented security controls. If it is discovered that no security control is in place for a particular asset and threat pair then a risk has been identified and a control can be implemented to reduce the risk. Another method of identifying risks involves relying on hindsight or looking in retrospect at previously documented security incidents as Lichtenstein (1996) mentions. This will provide insight about which assets were affected, which threats affected those assets and what organizational security weaknesses or vulnerabilities enabled these threats.

Risk Estimation

It is necessary to determine the likelihood of the occurrence of a threat once every risk has been exposed based on the vulnerability of the organization. It is vital to determine the perceived consequences an organization would experience as a result of the loss of assets due to some risk. Frosdick (1997) highlights several exercises which can be performed to satisfactorily estimate the probability of occurrence and consequences of each identified risk. Firstly, in estimating the probability of risks it is necessary to examine data concerning each specific threat with regard to its possible frequency of occurrence. This exposes vulnerabilities and facilitates accurate judgments regarding the probabilities of the occurrence of incidents resulting from risks at an organizational level and an inter-organizational level. It is necessary to apply common sense when estimating organizational vulnerability and the probability of risks producing negative impacts on an organization. Wold and

Shriver (1997) state that it is important to consider the following:

- Geographic position;
- Topography of a specific location;
- Ease of access to organizational facilities;
- Proximity of sources of power, water and airports;
- Access to local services provided by other companies in a region;
- How prone a particular area is to natural threats.

It is often challenging to estimate the probability of risks resulting in some negative impact. This could be because of a lack of sufficient information about particular risks but does not suggest that certain risks are of negligible importance. In situations such as this it is necessary to attempt to speculate the possible likelihoods of occurrence particular risks afford in resulting in some negative consequence. Once organizational vulnerabilities and the probabilities of risks have been established, the next step is to determine the possible consequences of such risks. Ascertaining the consequences of a certain risks may rely on speculation because there may be insufficient information to make an accurate estimation in this regard. For example, if IT-dependent business processes became unavailable because of a virus attack it may not be very easy to determine the extent of the damage. The primary reason for this situation is that it is not that easy to correctly estimate the exact value of intangible assets (Gerber & von Solms, 2001). Ultimately it is simpler to determine the expected losses incurred due to other risks, such as theft or vandalism of physical assets. These consequences may be quite evident because they are represented by the costs involved in the replacement of those assets. The consequences of a risk is determined by investigating the interdependency of the individual organizational components. For instance, if the IT department were to encounter various technical difficulties, the repercussions have the potential to ripple throughout the whole organization because all the departments rely with varying degrees of dependence on IT. An incident such as this may potentially manifest on a much larger scale. For example if one particular part of a supply chain were to experience some

negative impact causing it to be unable to function, all other reliant parts of the supply chain may be affected. Once the probability and consequence of a risk have been determined, these two pieces of information produce an indication of the potential a risk has to cause harm to an organization.

Risk Evaluation

It is then possible to commence with the final step in a Risk Analysis exercise, the evaluation of risk, once the potential for each risk to negatively impact on an organization has been appropriately estimated in terms of probability and consequence. Humphreys et al. (1998) states that the evaluation of risks makes it possible to distinguish between risks that are tolerable and intolerable. A more formal means of evaluating risks is by utilizing a risk matrix. Risk matrices enable the prioritization of risks from those that are most critical to those that are least critical. This prioritization is based on the value of the assets, the level to which each threat presents a danger and the level to which an organization is vulnerable to those threats.

Humphreys et al. (1998) describes the implementation of risk matrices in detail. Firstly, the value of each asset, the level of danger the threats pose to that asset and the level of vulnerability of the particular organization to the corresponding threat are plotted on the matrix. This gives an indication of the criticality of each individual risk. Once this criticality has been established, these risks can then be prioritized in list form based on the readings from the risk matrix. It becomes evident which risks an organization needs to pay considerable attention too, which ones they need to mildly consider and those they can disregard. It is not evident what an organization should consider as a tolerable risk and it is ultimately a decision for the organization itself. This was previously defined as the risk appetite of an organization which is unique to each organization based on their security needs. Strutt (1993) claims that the acceptance and tolerability of risks depends significantly on the beliefs, feelings and judgments of those involved in the risk assessment. Besides personal choice though, the acceptance of the consequences of particular risks should be made on a practical basis. As mentioned before it is more beneficial to implement risk-reducing measures only if the costs of their implementation are less than the benefits gained from their implementation.

An organization has a list of risks ranked in order of severity once a Risk Analysis exercise has been successfully completed. Risk Analysis has facilitated Risk Management by providing the information that enables the selection of appropriate security controls. It is possible to reduce the probability of a risk resulting in negative consequences but, it is important to remember it is not possible to completely remove a risk. There will be some residual risk that remains (Humphreys et al., 1998), even after precautionary measures have has been taken to adequately address such risks.

The type of information that a Risk Analysis produces may vary slightly depending on the type of assets and threats that are identified. This is because it is difficult to quantify the risks that affect intangible assets rather than those affecting tangible assets. Risk Analysis may be conducted by means of applying either quantitative or qualitative approaches or a combination of both.

Quantitative Risk Analysis

Bandyopadhyay et al. (1999) describes quantitative Risk Analysis as "based on expected value analysis, i.e. they assign dollar values to the various risks using probability theory". This "dollar value" refers to any currency relevant to a specific organization. Quantitative Risk Analysis can be conducted by calculating Annual Loss Expectancy (ALE), implementing the Livermore Risk Analysis Methodology (LRAM) for example. Livermore Risk Analysis Methodology (LRAM) will be discussed in greater detail to illustrate how a quantitative approach can be applied to facilitate IT Risk Management. The quantification of risk is not exact because there may be insufficient information available concerning the potential hazards that computer systems face (Turn, 1986). Those involved in analyzing any associated risks are required to speculate the effects of potential risks based on their own beliefs and opinions (Turn, 1986). Hence, quantitative Risk Analysis may contain an element of subjectivity.

Qualitative Risk Analysis

The process of qualitative Risk Analysis categorizes risks on a descriptive level using words i.e "Low" to "Medium" to "High" (Blakley et al., 2001).

A Risk Management approach relying on qualitative Risk Analysis techniques includes the CCTA's Risk Analysis and Management Methodology (CRAMM). This approach makes use of survey questionnaires and fuzzy logic to identify and assess risks. CRAMM will be discussed in more detail to illustrate how qualitative Risk Analysis methods facilitate IT Risk Management. Qualitative Risk Analysis attempts to formalize the subjective values placed on intangible assets and alleviate the mistaken sense of accuracy arising from quantitative Risk Analysis exercises (Gerber & von Solms, 2001). This is achieved using lookup tables that provide impact values based on the likelihood of threat occurrence (Gerber & von Solms, 2001). Qualitative Risk Analysis is to an extent limited by a lack of high-quality information required to sufficiently manage risks (Blakley et al., 2001). Therefore, it can be considered quite subjective.

The results of a Risk Analysis exercise, whether quantitative or qualitative, are all the same i.e. a list of risks prioritized in order of their criticality to an organization which can be appropriately dealt with through some IT Risk Management strategy. It can be a lengthy and time consuming task to conduct a Risk Analysis and Risk Management activity and these processes are often aided by automation. This helps risk managers conduct risk assessments and execute Risk Management activities with greater ease. These automated approaches to Risk Management are called Risk Management Software Packages. The National Institute of Standards and Technology (NIST) together with the National Computer Security Center (NCSC) have published the Risk Management Research Laboratory Overview (2003). This overview evaluates several Risk Management packages with the intention of undertaking research in Risk Management techniques and methodologies to outline the attributes and potential of such techniques. It is apparent that many of these packages use databases listing possible security controls , and those containing lists of threats and security incidents. These packages include data collection facilities in the form of questionnaires and surveys that assist in the generation of accurate results. Reporting facilities and graphical representations of output results are available. Most of these packages utilize either qualitative or a combination of qualitative and quantitative techniques. One drawback is the level of expertise required to complete the process effectively. However, to provide a general idea on how these packages may be

implemented to analyze risks and recommend security controls, several of the techniques will be discussed.

3.4 Information Technology Risk Management in Practice

There exist many ways in which various Risk Analysis and Risk Management strategies may be implemented through the application of quantitative and qualitative techniques. Two of these techniques were mentioned earlier, Livermore Risk Analysis Methodology (LRAM) and the CCTA's Risk Analysis and Management Methodology (CRAMM) and will be discussed in more detail.

3.4.1 Livermore Risk Analysis Methodology (LRAM)

Livermore Risk Analysis Methodology (LRAM) is an example of an IT Risk Management methodology employing quantitative Risk Analysis. The Risk Management Research Laboratory Overview (2003) describes LRAM as having two main objectives. These include identifying critical risks organizational risks and establishing the feasibility of currently implemented security safeguards and future ones. LRAM consists of three phases namely:

- Defining the scope of the exercise and establishing the resource and workforce requirements;
- Identifying assets, threats and the resulting risks as well as possible controls to reduce these risks;
- Prioritizing and selecting security safeguards based on a cost-benefit analysis.

Baskerville (1993) states that LRAM employs three specific metrics to fulfill its intended purpose. These include maximum potential loss (MPL) values that assist in the establishment of threat consequences. Secondly, loss potential indicator (LPI) values that are products of MPLs and quantifications of the possibility of safeguard failure, are used to establish the severity

of risks that could be detrimental to an organization's survival. Finally, cost-benefit ratios (CBR) are calculated as products of LPIs and threat frequencies and are used to determine the viability of new security safeguards. Such quantitative methods have declined in popularity due to their inflexibility and diminishing capability in achieving reasonable results. This is because it has become progressively more difficult to quantify the exact values of the tangible and intangible assets of an organization accurately. Qualitative methodologies for IT Risk Management were developed to formalize estimated assets values and the assumed criticality of potential IT-related risks. However, due to the inability to assign values to certain assets accurately such values may be assumed to hold some level of subjectivity.

3.4.2 The CCTA's Risk Analysis and Management Methodology (CRAMM)

The CCTA's Risk Analysis and Management Methodology (CRAMM) is a Risk Analysis and management methodology accepted by the UK government's Central Computer and Telecommunications Agency (CCTA). It employs Risk Analysis in a qualitative sense to assess and aid managing IT-related risks. A CRAMM review consists of three stages. These include:

- Identification and valuation of assets;
- Identification of threats and vulnerabilities and the calculation of risks;
- Identification and prioritization of security countermeasures.

The identification and valuation of assets is achieved by conducting interviews with data owners. They are asked to qualitatively estimate the values of assets by attempting to speculate on the potential impacts of associated threats. The identification of threats and vulnerabilities and the calculation of risks is the next stage. During this phase of a CRAMM review the potential likelihood of the occurrence of particular threats are determined based on any identified vulnerabilities that expose the assets. CRAMM achieves this by employing lookup tables for threat/asset groups and threat/impact combinations (Yazar, 2002). The risks affecting these assets can be appropriately analyzed once identified threats and vulnerabilities of assets have been

assessed. This is achieved employing a risk matrix with predefined values used to compare asset values against the identified and estimated threats and vulnerabilities (Yazar, 2002). The CRAMM software generates reports that highlight threat and vulnerability levels, based on the information produced by the identification of risks, to aid its final stage. This information is used by the CRAMM system to recommend the necessary countermeasures that will best address the identified risks. Additional reports are produced highlighting the most appropriate security controls along with the viability of implementing them in terms of there necessity and cost (Yazar, 2002). A CRAMM review provides an organization with an effective means of addressing IT-related risks. CRAMM does have some disadvantages. Firstly, it requires analyst expertise and can only be used by personnel with CRAMM experience. Another disadvantage is that the more detailed analysis of high risk assets can be lengthy, lasting up to several months (Gamma Secure Systems Limited, 1997).

It is important that an organization identifies its methods of implementing IT Risk Management to mitigate the risks associated with IT dependence. The final result is that the most pertinent aspects of organizational IT-related risks will be brought under control. It is necessary to stress the importance of implementing IT Risk Management to demonstrate its usefulness for reducing IT-related risks to an acceptable level and ensuring that the organization is appropriately upholding shareholder expectations.

3.5 The Importance of Information Technology Risk Management

Many organizations attempt to address the risks resulting from IT dependence. It is important that they employ well-structured Risk Management methodologies to get reap the benefits of their IT Risk Management activities, therefore, the necessity of IT Risk Management should be discussed.

3.5.1 The Necessity of Information Technology Risk Management

The management of the security of organizational computer systems is an important function (Whitson, 2003). There are new threats that are constantly becoming apparent and activities such as policy development, intrusion detection, monitoring, patching software and updating firewall rules prove to be an ongoing concern (Whitson, 2003). An effective approach to IT Risk Management however, can greatly facilitate the execution of these activities by providing the correct information about which important risks need to be addressed and thus ensuring that the correct controls are implemented. According to Kontio, Getto, and Landes (1998) major problem that currently exists is that not many organizations are implementing efficient and accepted Risk Management methodologies. The personnel involved in analyzing and controlling risks rely on their own intuition instead of attempting to manage risks by some structured and consistent methodology (Kontio et al., 1998). Kontio et al. (1998) suggests that "leaving Risk Management up to intuition and initiative may sometimes work but is a poor substitute for a systematic, professional and consistent approach for Risk Management". A sound and efficient approach to Risk Management provides a solid basis for identifying and controlling organizational IT-related risks. This is important because senior management must authorize their IT systems prior to their operation (National Institute of Standards and Technology, 2001). They are responsible for protecting the organization's IT assets and the mission of the organization (National Institute of Standards and Technology, 2001). The failure to adequately fulfill this responsibility could lead to negative consequences including the tarnishing of the corporate reputation and the loss of consumer and investor trust. It is imperative that senior management make every effort to ensure that all significant risks are identified and are fully addressed and identify other controls that may be needed to reduce IT-related risks (National Institute of Standards and Technology, 2001). It is important that residual risks are reduced to an acceptable level before the IT systems are authorized for operation otherwise the Risk Management process should be reiterated until this residual risk is at an acceptable level (National Institute of Standards and Technology, 2001).

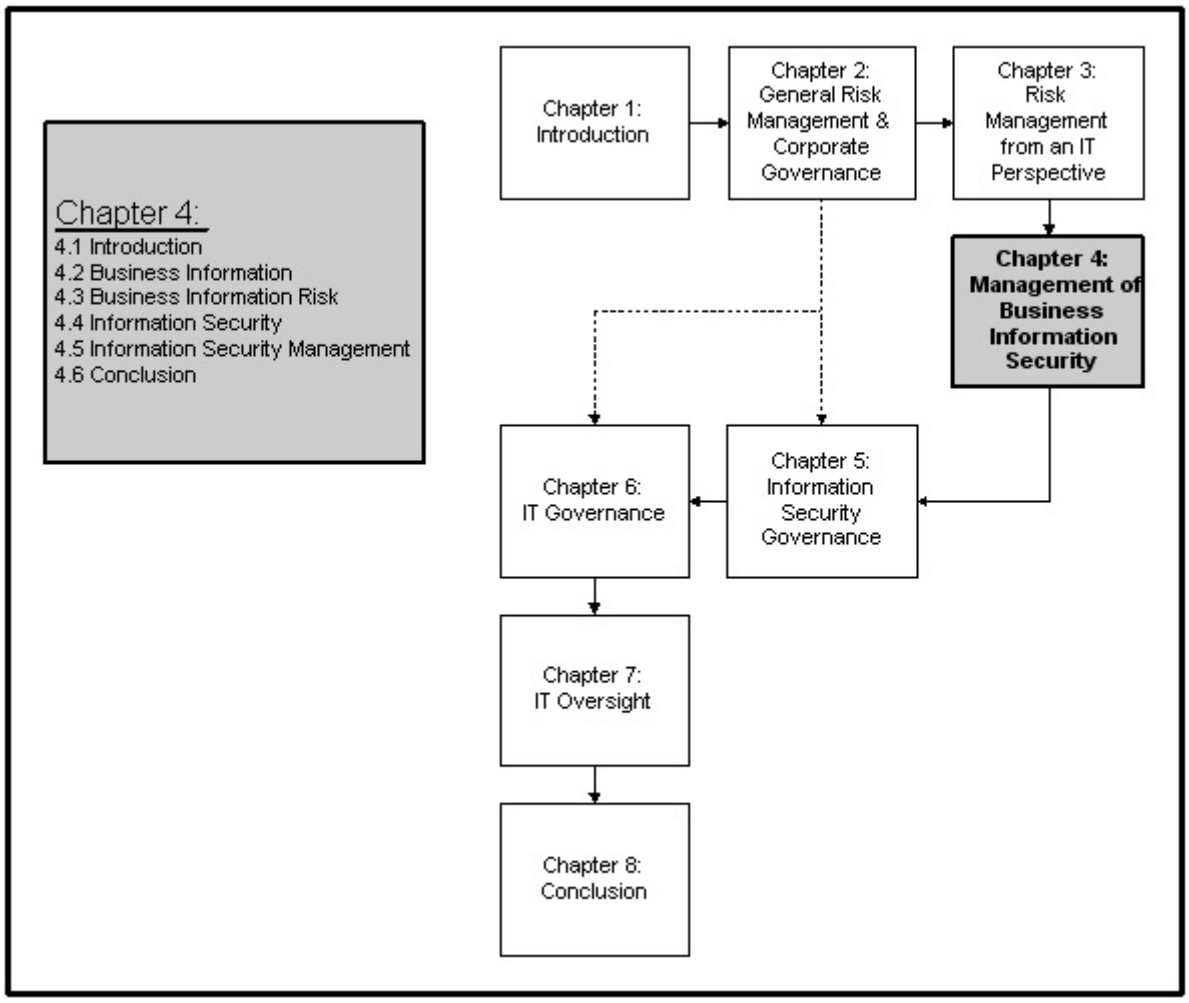
The implementation of IT Risk Management in a structured and appropriate manner ensures the best security controls will be implemented. Some benefits of correct control selection include removing various vulnerabilities of the IT systems, introducing a target control to mitigate the potential and driving force behind a threat as well as mitigating the enormity of the impact of particular risks (National Institute of Standards and Technology, 2001).

3.6 Conclusion

The importance of IT Risk Analysis and Risk Management are best demonstrated when considering the vast implementation of IT in an organization to facilitate the execution of business functions and providing competitive edge. The risks associated with IT will always be present and according to Bandyopadhyay et al. (1999) will only increase with dependence on IT. It would be impractical to believe that risk can be completely removed. The current business environment is all about how effectively risks are identified and managed. IT Risk Management should be a continuous process. This is important because the asset that is most at risk because of current organizational IT dependence is business information. IT enables competitive advantage through the effective use of business information resources. The use of IT has, however, exposed business information to numerous risks. It is essential that an organization make every effort to secure its business information. IT Risk Management has a role to play in this regard because it fits into the bigger framework of Information Security. Information Security ensures the proper protection of business information assets through the implementation of Information Security Management (ISM). The following chapter explores Information Security and Information Security Management to illustrate how information-related risks should be controlled.

Chapter 4

The Management of Business Information Security



4.1 Introduction

Business information plays a critical role in enabling most organizations to be successful and formidable industry competitors. IT greatly facilitates them in achieving this goal but exposes their information to a great variety of risks. IT Risk Management aims to mitigate these IT-related risks. However, this alone is not sufficient as the scope of business information risk is far wider that IT. Information Security aims to address the full scope of business information risks, through the effective implementation of Information Security Management. This chapter aims to motivate the importance of Information Security Management as the means by which business information risks are comprehensively addressed. The importance of business information is addressed and its scope and characteristics are defined. Business information risk, which involves more than IT-related risks, is discussed and he sources of such risks are noted. Information Security and Information Security Management are discussed to motivate their importance in terms of addressing the full scope of information-related risks.

4.2 Business Information

Business information is an important asset and exists in more than electronic form in most organizations. Business information is exposed to more than the technology that is used to transmit, store and process it. Therefore, it is necessary to define exactly what business information is and define its true scope. It is important to highlight some fundamental characteristics of business information and its importance as a corporate asset should be stressed.

4.2.1 Business Information Defined?

Information can be classified as some form of knowledge that is exchanged, and is represented by some particular type of data (OASIS, 2002). Normally, the everyday operations of most organizations involve dealing with a significant amount of business information. This business information is represented as anything from prospective business plans, financial records, customer lists and account details or contracts with business partners (Entrust,

2004a). Operational and support procedures and continuity plans are more examples (Humphreys et al., 1998) and market-related information about organizational products and services. These types of information can exist in a multitude of forms. Some examples include information stored on computers, in databases and data files, electronically conveyed through networks, email messages and web pages, stored paper documents, other printed, faxed or written paper documents, stored on tapes, CDs, DVDs and other disks or even conveyed by word of mouth through conversations and the use of mobile devices (Humphreys et al., 1998).

There are many threats that put business information at risk irrespective of what type of information is stored or communicated and the medium by which it is stored (Gordon, 2002). Information is exposed to these threats while it is exchanged and utilized during the daily business operations of an organization. Thus, to protect information effectively it is necessary to demonstrate its true scope.

4.2.2 The Scope of Business Information

Information Technology can play a major role in processing, transmitting and storing information. The development of private networks and the widespread use of the Internet help organizations to perform business transactions with customers, suppliers and business partners more efficiently (Entrust, 2004a). This has enabled organizations to extend their reach to provide services and collaborate with business partners in outlying markets.

Information Technology has benefited organizational personnel because the implementation of networks has enabled them to gain access to real-time information and computer applications that enable them to complete their daily business activities successfully (Entrust, 2004a). The utilization of technologies has helped satisfy the needs of the majority of organizational stakeholders who may require convenient access to information and business services. An organization should be able to deliver this if it wishes to remain a competitive force in industry. Such a situation requires that an organization share its business information resources more openly with its stakeholders, who may be distantly located.

The following scenario acts as an example. A retail store needs to replenish stock and purchases goods from one of its suppliers. This forms

part of its common business activities and requires that a certain amount of information is exchanged or "shared" between the two relevant parties involved in the transaction. This activity can be accomplished through an automated supply chain, like that of Wal-Mart. The company uses its existing Internet line to set up a connection between its own accounting system and that of the supplier (Carlton Collins, 2003). For the transaction to be completed successfully the two accounting systems must be able to communicate and exchange the relevant information required to purchase the goods from that supplier (Carlton Collins, 2003). This is accomplished by placing a purchase order through their accounting system with their supplier. The purchase would disclose information like company name and address, shipping address, terms, shipping method and detailed information about the stock being ordered (Carlton Collins, 2003). The purchase order is electronically submitted and captured into the accounting system of the supplier (Carlton Collins, 2003).

The accuracy of the information submitted via the purchase order is important, however, throughout such a business activity this information may fall susceptible to numerous risks. There is the possibility that a hardware or software failure may prevent the purchase order from reaching its intended destination or be corrupted in some way. Furthermore, through electronic transmission, the information may be intercepted by some unauthorized individual such as a hacker. The various business processes applied to process the information in the purchase order and successfully complete the transaction can present risks. This demonstrates that important business information is exposed to more than technology and the risks associated with its electronic storage, processing and transmission while an organization undertakes its various business activities.

Information is exposed primarily to three fundamental elements namely: people, processes and technology (ISO/IEC 17799, 2005). Nowadays, each of these elements plays an essential role in facilitating an organization in executing its key business operations. Therefore, the presence of information in any business operation does not mean that it is exposed to only a technology element. The scope of business information, from a risk point of view, includes consideration for the people and processes and technology that it comes into contact with.

Information needs to be protected from the various risks that each of these elements present for it to remain useful to an organization in its business operations. This protection involves preserving several fundamental characteristics that enables such information to retain its value to the organization.

4.2.3 The Characteristics of Business Information

Information plays a major role in supporting normal business operations in most organizations. It comes into contact with various people, process and technology elements during these business operations. These elements form an essential component of most business operations and have great potential to pose considerable amounts of risk to the business information. Therefore, to ensure that business information provides valuable support continuously through its effective use, it was stated that several key information characteristics require preservation. These include confidentiality, integrity and availability (ISO/IEC 17799, 2005).

Confidentiality

Humphreys et al. (1998) assert that maintaining confidentiality involves "protecting sensitive information from unauthorized disclosure or intelligible interception". Therefore, to preserve the confidentiality of information it must be kept secret. Sensitive business information should not be made freely available to whoever wants to gain access to it. Only those parties who have been given authorization to access this information should be allowed to do so. This includes a specific organization, a department within an organization or even a particular individual (Thomson & von Solms, 2003). Thomson and von Solms (2003) state that the confidentiality of information is preserved by applying either one of two approaches but preferably both. These include restricting access to confidential information or encrypting it.

Integrity

The preservation of the integrity of business information involves ensuring that its correctness and comprehensiveness is maintained (Humphreys et al., 1998). Information integrity is important because information plays a ma-

jor role in the decision making process (Ritchie & Brindley, 2001). Corporate executives risk making misguided business decisions if information is not accurate or complete. Ultimately these decisions could lead to unwanted situations in an organization, which could have been prevented. A breach of integrity may result from the intentional modification of information by unauthorized or unlawful parties. Integrity can be breached through unintentional modification while information is being stored, processed or transmitted (Thomson & von Solms, 2003).

Availability

The preservation of the availability of business information requires it to be made accessible for use, by those parties who need it, at the time when they need it. Ensuring availability is important because without timely information an organization would be incapable of continuing normal operations (Gerber & von Solms, 2001). This is because having the correct information at the right time enables management to make well-timed business decisions allowing an organization to gain a competitive advantage over competitors (Gerber & von Solms, 2001). One of the most common ways in which availability is compromised is through a denial-of-service (DoS) attack. During a DoS attack an information system is typically flooded with a large amount of information requests, which cannot be handled by the system, and it either slows down or malfunctions, making the information unavailable (Whitman & Mattord, 2003a).

The preservation of the characteristics of business information ensures that such information remains useful to an organization and its stakeholders. It is necessary to address the importance of business information retaining its value to clearly stress this point.

4.2.4 The Importance of Business Information

Towards the late nineties there was a growing perception that information can be viewed as an important resource and even as a commodity (Busch-Vishniac, 2001). Customers and suppliers wish to remain confident organizational honesty, ability to deliver, motivation to offer services and status in terms of financial stability (Thomson & von Solms, 2003). These stake-

holders wish to acquire products and services that are founded on a basis of trust (Busch-Vishniac, 2001). These products include information which is viewed as a commodity (Thomson & von Solms, 2003). Information is so important that some, including Halliday, Badenhorst, and von Solms (1996) state that "information has become the key resource and even the life blood of many organizations". Eloff, Labuschagne, and Badenhorst (1993) state that "information is the glue that holds an organization together and allows all other resources to be managed".

Information plays an integral role in how organizations conduct their daily business activities (Gerber & von Solms, 2005). The vast integration of IT, and use of computer networks and the Internet in business today, have enabled electronic commerce which has become a fundamental tool for enabling corporate survival and growth (Jung, Han, & Suh, 1999). This is because information is constantly shared between parties conducting business through electronic commerce-based transactions. Therefore, modern society is said to be mainly driven by information (URN 99/704 (NEW), 1999).

The proficient use of information has the ability to facilitate an organization in achieving competitive advantage. This helps produce business value and adequately fulfill shareholder and investor expectations.. The information provided to top executives guides them in making the numerous critical business decisions that form part of their daily responsibilities. Important business decisions can impact organizational strategy and should be based on information that is confidential, accurate and timely. If any of these characteristics have been compromised, the resultantly ill-advised decisions of Executive Management may have a negative impact on the business. Some negative effects include financial loss and the tarnishing of the corporate reputation (Entrust, 2004a). These consequences can serve as a mechanism to dissuade further investment. Incidents like these hint at the value and importance that should be attached to business information resources. It is important to understand business information risk to preserve the characteristics of business information by protecting it from these risks.

4.3 Business Information Risk

It is necessary to define what business information risks are and establish their sources.

4.3.1 Defining Business Information Risks

In the current business environment, for organizations to grow and continue to maintain a competitive advantage, they need to provide greater access to their information resources and business services (Entrust, 2004a). An example of this includes providing personnel with real-time access to computer applications and business information to increase productivity (Entrust, 2004a). Other examples include computerizing key business processes and business transactions with suppliers over the Internet to increase speed and cost savings, and facilitating customers in performing online transactions. This assists in enhancing customer service and increasing brand loyalty and revenues (Entrust, 2004a). All these activities require that vast amounts of information, which may be confidential, is shared. Such wide and open access to information and business services has the potential to create significant amounts of business information risk.

It becomes imperative that all business information risks are addressed when considering the fast rate of technological development and innovation that continuously makes conducting business much easier. Wills (1999) motivates that "the information society of the future will just not work if the information we rely on - the lifeblood of the business - is not secured". Therefore, it is important to understand and define where business information risks may stem from so that they may be addressed.

The risks that impact on information assets are categorized into two groups (Entrust, 2004a). The first group includes risks which have the potential to negatively impact on business information from outside the organization. The second group includes risks which jeopardize business information from inside the organization. However, irrespective of where the business information risks occur the fact remains that the risks in each of these groups present challenge to providing adequate protection for business information (Entrust, 2004a). For organizations to provide an adequate level of protection for their business information assets, it is important that they identify

the various internal and external risks.

4.3.2 Sources of Information Risk

There are many sources from which business information risks may arise both internally and externally to an organization. The risks from external sources may arise as a result of its industry competitors or hackers (Entrust, 2004b). Hackers use their knowledge of IT to commit fraud and attempt to illegally gain access to confidential information by bypassing the security controls put in place to protect it (Whitman & Mattord, 2003a). Internal sources of risks may arise as a result of inquisitive or discontented personnel or contractors (Entrust, 2004b). These persons may feel that they have been treated unfairly by a particular organization and seek to illegally gain revenge by causing some kind of damage.

It was mentioned in the previous chapter that there are three main sources of threats that may present risks to information. These are natural, human and technical or IT-related threats that cause risks. IT risks are important because IT is widely used to facilitate the use of information. Smith (1989) states that computers and related technologies form the "information backbone" of most organizations operating in the world today. However, the risks that arise from human sources seem to be the most frequent and damaging to business information assets. Some concerns relating to human risks involve the theft, modification, interception, and distribution of sensitive and private data and fraud (Entrust, 2004b). Such risks can result in damage to the corporate reputation of an organization and even cause a degree of financial loss (Entrust, 2004b).

All these risks ultimately seek to compromise the confidentiality, integrity and availability of business information. The quantification of the risk of data theft, according to Entrust (2004b), reveals that breaches of confidentiality result in disruptions over a lengthy time period, lasting longer than a month in some cases. Furthermore, the recovery from and investigation into such breaches involve considerable staff time generally around 10-20 days and requires significant financial resources (Entrust, 2004b).

The ensuring of the security of sensitive business information can be a significant challenge because information can be stored in different locations like files and folders on computer desktops, in laptop computers, and on

servers (Entrust, 2004b). Information may be duplicated and transferred between locations, whether these locations are within an organization or between the organization and other stakeholders such as customers, business partners or regulatory authorities (Entrust, 2004b).

Information Technology Risk Management efforts play a major role in addressing the IT-related risks that business information is exposed to. However, because the scope of business information is far wider than IT and the risks that affect it arise from human, natural and IT sources, IT Risk Management alone is not comprehensive enough to ensure that all areas of information risk are mitigated. Therefore, it is essential that organizations attempt to address all aspects of business information risk through the process of Information Security.

4.4 Information Security

Information Security is a fundamental organizational responsibility required to comprehensively secure vital business information assets. Thus, Information Security should be defined and its importance accurately stressed.

4.4.1 Information Security Defined

Humphreys et al. (1998) state that the principle function of Information Security is to maintain business continuity and reduce the consequences that cause harm to an organization by stopping or mitigating the influence of Information Security breaches. Information Security is the activity that aims to protect information from a broad spectrum of risks to optimize Return on Investment (ROI) and business opportunities (ISO/IEC 17799, 2005). Information Security aims to preserve the confidentiality, integrity and availability of business information to achieve this. These characteristics are preserved through the application of an appropriate set of security controls.

Security controls can include, as the IT Governance Institute (2005e) states, "a layered series of technological and non-technological safeguards such as physical security measures, background checks, user identifiers, passwords, smart cards, biometrics and properly implemented and managed firewalls". Security controls also include policies, practices, procedures, organizational structures, software and hardware operations (ISO/IEC 17799,

2005). Whitman and Mattord (2003b) maintain that security awareness, training and education are important to ensure that business information assets are adequately secured. All organizations should implement a range of security controls that aim to satisfy their Information Security requirements.

There are essentially three high-level Information Security requirements common to most organizations. These specifically include: first, the requirements to protect the IT infrastructure; second, the business requirements for Information Security, which depend on factors such as organizational size and the type of business the organization conducts, that need to be considered to preserve the confidentiality, integrity and availability of business information; and third, any legal, regulatory or statutory requirements related to the protection of information (ISO/IEC 17799, 2005). These legal and regulatory aspects of Information Security will be discussed in subsequent chapters. These requirements with the guidance of industry best practices and well-regarded security standards, such as ISO/IEC 17799 (2005), help an organization establish a foundation for an effective approach to Information Security. Information Security standards and best practices, such as ISO/IEC 17799, will be discussed later in this chapter.

Information Security needs to be an ongoing and repetitive exercise to ensure that an organization continues to fulfill its Information Security requirements. The IT Governance Institute (2005e) states that "in the ever-changing technological environment, security that is state-of-the-art today is often obsolete tomorrow. Security must keep pace with these changes. Security must be dealt with in a proactive and timely manner to be effective".

The objective of Information Security involves preserving the confidentiality, integrity and availability of information by applying an appropriate set of security controls that aim to fulfill the Information Security requirements of an organization. These requirements involve a lot more than merely considering IT-related issues. IT Risk Management plays a role in Information Security but only fulfills part of the Information Security needs. Since information security has been defined as the process through which all information-related risks are addressed it is necessary to discuss why it this is so important.

4.4.2 The Importance of Information Security

Information Security is important, not for its own sake, but for the influence it could have on an organization because there is a ROI that can be gained by successfully implementing Information Security (Deloitte and Touche, 2002).

Information is viewed as one of the last remaining competitive advantages that organizations can utilize (Thomson & von Solms, 2003). If information is not exploited responsibly the consequences involve the tarnishing of the corporate reputation or ultimately even its demise (Msomi, 1999). Preserving the confidentiality, integrity and availability of business information through sound Information Security efforts is important to sustain competitive edge, cash-flow, profitability, legal compliance and corporate image (ISO/IEC 17799, 2005).

It is important to protect information systems, which play a major role in managing business information assets to secure information effectively. Their effective use can lead to numerous direct and indirect benefits, such as those mentioned above (Williams, 2001). Conversely, these information systems, if not appropriately protected, can also generate many direct and indirect risks (Williams, 2001). Such risks have the ability to cause a gap between the amount of security that is employed and the actual need to protect information systems and information (Williams, 2001). The IT Governance Institute (2005e) lists several factors that cause such a gap. These include:

- The enterprise-wide implementation of technology;
- The interconnectivity of information systems;
- The bypassing of constraints such as distance, time, and space;
- An unevenness of technological innovation and change;
- The decentralization of management and control;
- The allure of carrying out unconventional cyber attacks against organizations;
- External considerations like legal, regulatory or even legislative requirements and advances in technology.

The interconnecting of public and private networks and the sharing of sensitive business information can make access control difficult (ISO/IEC 17799, 2005). This is because the progression towards networked computing has undermined the usefulness of centralized, professional control (ISO/IEC 17799, 2005). This has highlighted the need for effective Information Security which should be implemented at every point in a distributed computing environment. Advances in technology, such as the development of public and private networks, have the potential to improve key business operations, therefore, enhanced and well developed Information Security efforts help generate business value (ISO/IEC 17799, 2005). The generation of business value is achieved through Information Security that contributes towards dealings with business partners, closer customer relationships, better competitive advantage and a stable corporate reputation (ISO/IEC 17799, 2005).

Traditionally, information systems have not been designed with security in mind (ISO/IEC 17799, 2005). The Information Security efforts that are implemented via technical measures are limited in scope and should be sustained by appropriate management and procedures (ISO/IEC 17799, 2005). Scant consideration for Information Security in systems design means that effective Information Security efforts are critical. A lack of security will affect the ability of the organization to reach its full potential in terms of business success and could cause it to experience the consequences of legal or regulatory non-compliance.

All types of organizations, big or small, from global enterprises to the smallest Small to Medium Sized Enterprises (SME's), are susceptible to the security risks associated with business information (Humphreys et al., 1998). The identification and implementation of appropriate security controls through effective Information Security is essential. Prompt attention to protecting business information will reduce the costs and increase the efficiency of Information Security efforts (Humphreys et al., 1998). Information Security implemented in this way, will add to the development of new and easier means of handling online business transactions and building trusting stakeholder relationships. There are several key risk areas that an organization needs to consider to implement Information Security appropriately and create a trusting environment between itself and its stakeholders. The IT Governance Institute (2005e) states that such areas of risk could have a

considerable influence on business operations and include:

- Heightened requirements for availability and robustness;
- Increasing possibilities for the unethical exploitation of information systems which has an impact on privacy;
- Outside threats from hackers, which may result in denial-of-service or even virus attacks, extortion and the unethical dissemination of sensitive business information.

All these risks demonstrate the need for proper Information Security efforts. These are put into practice through the process of Information Security Management (ISM).

4.5 Information Security Management

Information Security Management is the process that exemplifies the implementation of Information Security. There is a need to define what Information Security Management is and explain how it can be implemented. What the process of Information Security Management entails should also be illustrated.

4.5.1 Information Security Management Defined

Information Security Management is the process of carrying out various activities that facilitate the preservation of business information. It is an expression of Information Security objectives that aim to fulfill the Information Security requirements of an organization. These security objectives are communicated through the Corporate Information Security Policy (CISP). Information Security Management involves implementing security measures that exemplify the instructions contained in the CISP, various security procedures and other security programs (Whitman & Mattord, 2003a). The CISP will be discussed in subsequent chapters.

Repetition and review are key features of the Information Security function. Information Security Management is a continuous process and requires constant review and adjustment to keep it abreast with the latest technological developments and their associated risks (Whitman & Mattord, 2003a).

According to Whitman and Mattord (2003a) Information Security Management can consist six consecutive phases. These include investigation, analysis, logical design, physical design, implementation and maintenance and change.

During the ***investigation*** phase the various costs of implementing a security program are estimated and all the available resources of the organization are evaluated (Whitman & Mattord, 2003a). This helps to assess the feasibility of the project and enables an organization to plot the scope of their Information Security Management program. An additional feature of the investigation phase involves setting the Information Security goals which are recorded in the corporate information security policy (Whitman & Mattord, 2003a).

The ***analysis*** phase commences next and entails an investigation of the effectiveness of existing Information Security policies and security programs. Other typical activities carried out include an assessment of threats and the effectiveness of implemented security controls (Whitman & Mattord, 2003a). An organization conducts a Risk Analysis exercise during this phase to identify, estimate and evaluate its Information Security risks (Whitman & Mattord, 2003a). This helps the organization to identify its Information Security requirements, which include consideration for its business needs for security, IT infrastructure-related requirements and legal issues.

The ***logical design*** phase follows the analysis phase. During this phase an organization establishes whether or not it should continue to implement the security project on its own or decide to outsource to external consultants and security experts. Typical activities characteristic of the logical design phase include the development of the Information Security "blue print" and incident response planning to help mitigate and remediate potential disasters (Whitman & Mattord, 2003a).

The ***physical design*** phase commences next and during this phase the various technologies needed to support the Information Security "blue print" are selected for implementationa. Additionally, the physical security measures required to sustain the selected technological solutions are designed and the entire security project is reviewed and approved (Whitman & Mattord, 2003a).

Once the Information Security project has been designed and the appro-

priate means are selected to implement the project, the ***implementation*** phase commences. During this phase an organization either purchases or develops the elements required to implement security based on the established security "blue print" (Whitman & Mattord, 2003a). Once this phase nears its completion the security solution is presented to management who are required to finally approve it (Whitman & Mattord, 2003a).

This final phase is ***maintenance and change***. During this phase an organization continuously monitors, tests, adjusts, updates and repairs its Information Security Management System (Whitman & Mattord, 2003a). This enables the organization to remain up-to-date with the latest security risks that result from the constantly changing business environment in which it operates.

The primary intention of an Information Security Management program is to identify threats and create and implement security controls that counteract those threats (Whitman & Mattord, 2003a). An organization needs to ensure that it has sufficient guidance about how Information Security should be managed and implemented to accomplish this effectively.

4.5.2 The Implementation of Information Security Management

The National Security Telecommunications and Information Systems Security Committee document title the National Training Standard for Information Security Professionals NSTISSI No. 4011 portrays an all-inclusive model for Information Security (Whitman & Mattord, 2003a). This model, more commonly known as the NSTISSC model, is growing in importance to become the evaluation standard for information systems security (Whitman & Mattord, 2003a). It presents three dimensions that can be considered equally important when securing both information and information systems effectively.

The first dimension of the model represents the confidentiality, integrity and availability of information. The second dimension represents the states of information i.e. whether it is in storage, processing or transmission. The third dimension represents three key controls required to secure information, namely, policy, education and technology. These dimensions are mapped out

against one another, resulting in a 3 x 3 x 3 cube with 27 cells characterizing the various aspects that need to be addressed to secure information and information systems successfully (Whitman & Mattord, 2003a). Whitman and Mattord (2003a) illustrate that an intersection between the technology, integrity, and storage aspects, for example, demonstrates the need for a technological security control that preserves the integrity of business information whilst it is in storage. All organizations should attempt to satisfy the criteria in these cells to a level that is acceptable to them. This ensures that their security efforts are at a standard that portrays them as trustworthy business partners.

Organizations need guidance about which controls are the most effective to gain assurance that they have addressed all aspects of security presented in the NSTISSC model to achieve this. They should use accepted industry standards and codes of practice that recommend proven Information Security controls and adequately address Information Security. Information Security standards and codes of practice are important because they are used to promote global Information Security principles and nurture trusting relationships between an organization and its stakeholders (Gerber & von Solms, 2001). ISO/IEC 17799 is an example of a standard that offers guidance on how to approach Information Security through means proven to work in many organizations. ISO/IEC 17799 is only one approach to Information Security Management and there are several others that can be implemented. ISO/IEC 17799 serves as a starting point for organizations to begin an effective Information Security Management strategy (ISO/IEC 17799, 2005).

ISO/IEC 17799, was compiled by the Joint Technical Committee ISO/IEC JTC 1, Information Technology, Subcommittee SC 27, IT Security Techniques (ISO/IEC 17799, 2005). ISO/IEC 17799 "sets out guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization. It contains best practices regarding control objectives and controls in information security management" (ISO/IEC 17799, 2005).

ISO/IEC 17799 comprises 11 security control clauses which contain 39 main security categories and one introductory clause presenting risk assessment and management (ISO/IEC 17799, 2005). The various security control clauses in ISO/IEC 17799 are:

1. Security policy;
2. Information Security organization;
3. Assets classification and control;
4. Personnel security;
5. Physical and environmental security;
6. Communications and operations management;
7. System access control;
8. Information systems acquirement, development and maintenance;
9. Incident Management;
10. Business continuity planning;
11. Compliance.

The various security controls across these control clauses may, however, not be suitable for every corporate milieu and should be implemented discerningly, with respect to local business conditions, which determine security requirements (ISO/IEC 17799, 2005). It is up to each organization to decide which security controls they require, based on the level of risk acceptance, risk treatment alternatives, and the broad Risk Management strategy of the organization (ISO/IEC 17799, 2005). An initial assessment of the risks an organization faces, in terms of its business information assets, helps determine which security controls are the most applicable. ISO/IEC 17799 recommends ten key security controls considered relevant to every business in every organizational context (ISO/IEC 17799, 2005). The controls are derived from fundamental requirements, such as those stipulated by legal and regulatory authorities, or are considered common practice for Information Security (ISO/IEC 17799, 2005). These ten key security controls are:

1. Protection of data and personal information privacy;
2. Organizational record protection;
3. Intellectual property rights;

4. Security policy document;
5. Delegation of roles and responsibilities for Information Security;
6. Information Security awareness, training and education;
7. Accurate processing in applications;
8. Vulnerability management;
9. Business continuity planning;
10. Information Security incident management.

A document such as ISO/IEC 7799 enables an organization to promote itself as a trustworthy business partner, by demonstrating internationally approved means of addressing the broad spectrum of Information Security risks. Information Security Management involves numerous activities that help an organization to apply Information Security effectively, aided by ISO/IEC 17799. Additionally, ISO/IEC 27001 is a specification for an Information Security Management System that forms the basis for third party audit and certification defined according to ISO/IEC 17799. It is important to explore the process that is followed to implement an Information Security Management program effectively in more detail.

4.5.3 Information Security Management: The Process

Information Security Management begins with a clear direction. Information Security standards and codes of practice provide an organization with the assurance that it has covered all important aspects of business information risk in a manner that meets international expectations. These organizations can then be considered trustworthy business partners. The issuing of a CISP helps to express the commitment of the organization towards protecting the confidentiality, integrity and availability of business information. Once the CISP has been compiled and clearly states their Information Security objectives, various Information Security activities commence to accomplish these objectives. Some of these activities include an initial assessment of potential risks to information followed by some Risk Management strategy. This enables an organization to identify, select and implement an assortment of

appropriate physical, technical and operational security controls based on the guidance of standards such as ISO/IEC 17799 and legal and regulatory requirements. Other activities that are carried out through an Information Security Management program include staff training in security practices, testing the security infrastructure, detecting and responding to various security incidents and business continuity planning (Entrust, 2004a). Other key elements are auditing the security function and reporting to Executive Management on its effectiveness which promote accountability and responsibility for the broader Information Security function.

Information Security Management is a very important function in any organization. It is paramount that all organizations attempt to address Information Security in an appropriate manner. This ensures that business information is adequately preserved and organizations exploit it in a responsible way that produces competitive advantage and satisfies shareholder expectations.

4.6 Conclusion

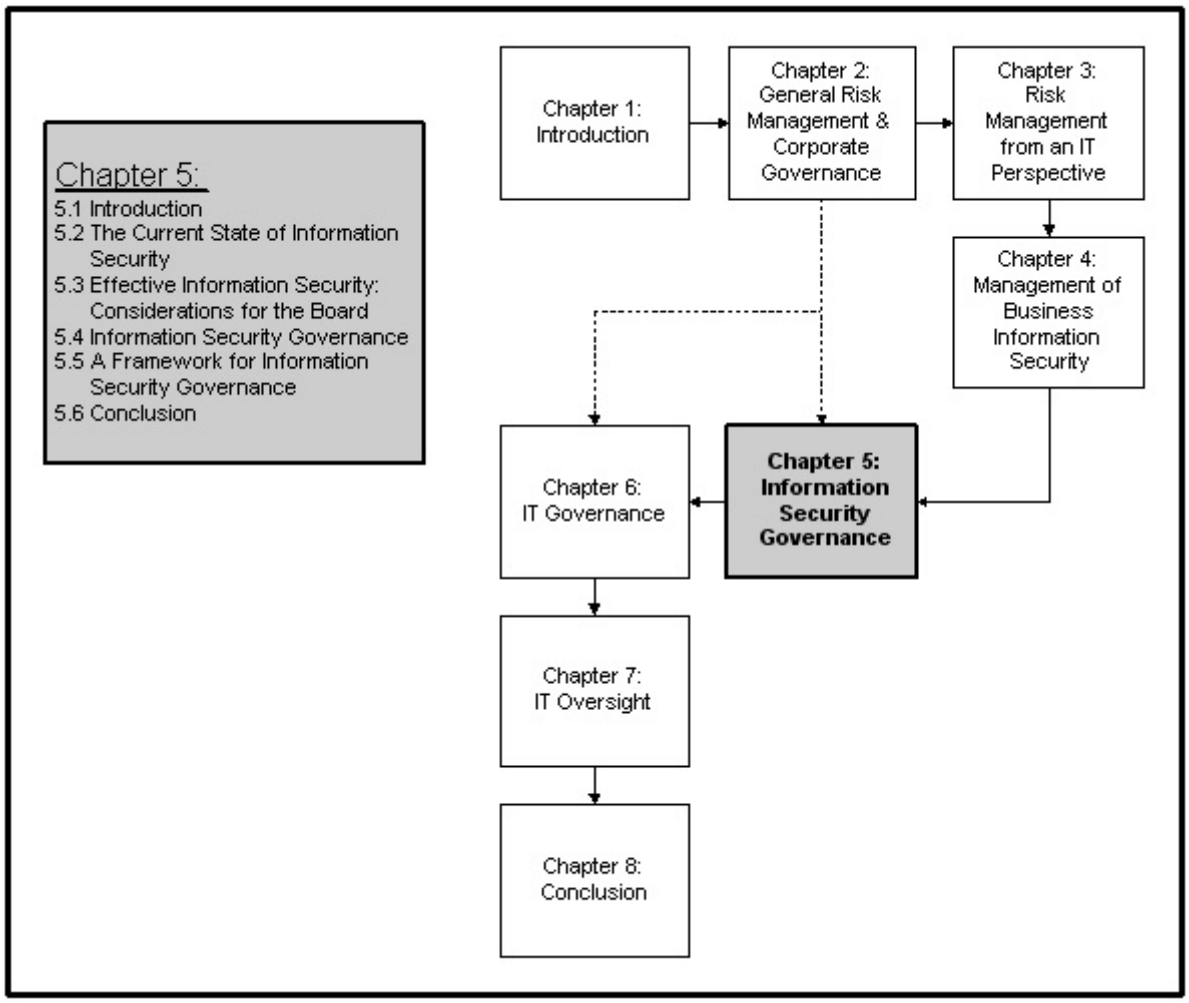
Information Security Management is vital to preserve the confidentiality, integrity and availability of information effectively across the broad spectrum of information-related risks. This includes consideration for various people, process and technology elements. Thus, the Information Security Management function helps an organization fulfill its necessary Information Security requirements. This demonstrates that such an organization is able to exploit information responsibly to create business value and generate shareholder returns and can, furthermore, be considered a trustworthy business partner. It is the responsibility of the BoD to ensure that the interests of the shareholders are satisfied. Since the effective use of information is key to creating business value and generating shareholder returns, Information Security should be a board-level responsibility. However, currently Information Security seems to lack board-level attention (Business Software Alliance, 2004). Thus, it should become an important part of Corporate Governance and a responsibility of the BoD through sound Information Security Governance efforts.

Part III

Solution

Chapter 5

Information Security Governance



5.1 Introduction

Information Security Governance is important to ensure the BoD is involved in the corporate Information Security function. This ensures that an organization is able to set an accurate Information Security strategy which can be exemplified through an effective Information Security Management function that is aligned with its goals, business objectives and needs for security. This chapter aims to demonstrate the need for Information Security Governance (ISG) and proposes a framework to guide the BoD in its organization-wide implementation. The need for ISG is demonstrated by highlighting several important concerns about the manner in which the corporate Information Security function is currently addressed and why there is a need to rethink that way it is executed. Various important considerations that the BoD should be aware of in terms of Information Security are discussed to demonstrate the need for board-level involvement in the corporate Information Security function. These considerations demonstrate board-level accountability for Information Security and necessitate the need for ISG. Consequently, ISG is discussed in detail explaining what it aims to accomplish and why the BoD should consider it. The framework for ISG is proposed to guide the BoD in their ISG endeavors and it is justified by demonstrating some of the benefits of implementing ISG.

5.2 The Current State of Information Security

The importance of Information Security as a key business responsibility cannot be stressed enough. Every organization should attempt to implement Information Security effectively. The assurance that the corporate Information Security function is indeed effective needs to be scrutinized in detail. Therefore, any problems with Information Security should be elucidated and the way Information Security is approached needs addressing.

5.2.1 Problems with Information Security

Fewer than four out of ten consumers trust that most organizations manage their information in a proper and confidential way, according to a survey carried out by Gordon and Glickson (2001). This perception could discourage investment if appropriate Information Security practices are not implemented. Therefore, implementing appropriate means to protect information will protect the organization (Gordon & Glickson, 2001).

There needs to be a commitment from everyone in the organization to fulfill their role in terms of Information Security to protect information adequately. This includes the active engagement of the BoD and senior management and includes employees at all levels in the organizational structure. However, a major concern in most organizations is that the BoD and senior management do not demonstrate responsibility or commitment to Information Security (von Solms, 2001). This makes it difficult for the Information Security Officer (ISO) to manage Information Security on an organization-wide basis (von Solms, 2001).

The Business Software Alliance (2004) highlights two critical obstructions which hinder effective Information Security. Firstly, the responsibility for Information Security is frequently handed over to the Chief Information Officer (CIO), or the Chief Security Officer (CSO), who may not necessarily be positioned to delegate the resources and have the authority required to resolve various Information Security-related issues (Business Software Alliance, 2004). Due to this lack of attention by Executive Management the allocation of finance to Information Security efforts is scant in relation to the risks and degree of damage that security incidents may produce (Business Software Alliance, 2004). Secondly, many handbooks exist offering technical assistance and general principles of Information Security (Business Software Alliance, 2004). Nonetheless, there is still no accepted, standardized enterprise-level framework to resolve what must be accomplished and by whom (Business Software Alliance, 2004). This lack leaves organizations in a situation where they remain doubtful about how to apportion financial and other resources for security and effectively measure the business value to be gained by such investments (Business Software Alliance, 2004).

A major point of concern stems from the fact that frequently at an Executive Management-level and board-level Information Security is often per-

ceived as a technology issue (Entrust, 2004a). This clarifies why Information Security is handed over to the IT department with little further concern (von Solms, 2001). The CSO and other security personnel are confronted with an arduous task in executing the Information Security program and considering the various Information Security components of the organization without the necessary support of top executives (von Solms, 2001). These security components may include policy, awareness, human, legal and assessment and monitoring (von Solms, 2001).

Citadel Security Software, Inc. (2005) highlights several factors that demonstrate the problems with Information Security because it is viewed from a technical point of view at a tactical level in the organization. These factors demonstrate that security is:

- Reactive rather than proactive i.e. it concentrates on the identification of and response to threats;
- Project-driven as opposed to policy-driven;
- Not aligned with the business goals and objectives of the organization;
- Poorly coordinated across organizational borders.

These issues present some very real concerns that organizations should consider. There is a need to rethink the way security is addressed to adequately protect business information assets and nurture trusting relationships with business partners and customers.

5.2.2 Addressing Information Security

It is important to consider the various Information Security requirements that were discussed in the previous chapter to demonstrate how Information Security can be implemented effectively. These security requirements stem from sources both internal and external to an organization. The significance of properly addressing these security requirements is essential to avoid the consequences resulting from negligence in terms of Information Security.

Internal security requirements include those needed to protect the IT infrastructure. Chapter Three discussed what is necessary to address such

IT-related risks in depth. Additionally, there are the requirements for information integrity, confidentiality and availability as identified by an organization's business needs. Humphreys et al. (1998) describe these business requirements as those which complement an organization's company-wide principles, goals and needs in terms of information processing that will sustain its normal business operations.

There are various legal, regulatory and statutory obligations, in terms of external security requirements, that are imposed on organizations by governments and other regulatory authorities. These legal requirements shall be discussed later in this chapter. Other external requirements include consideration for the guidance of accepted security standards, such as ISO/IEC 17799 (2005). It is important to consider standards and best practices. The adoption of these standards and best practices enables an organization, in many cases, to undertake a certification process that demonstrates that it follows an accepted approach to Information Security and can be considered trustworthy. Consideration for standards and best practices and security requirements discussed helps an organization establish a basis for an effective approach to Information Security.

These internal and external security requirements help address the various important aspects of business information risk that most organizations face. Figure 5.1 illustrates the relationship between these various internal and external security requirements which mitigate the numerous internal and external risks affecting business information.

Information Security is a complex issue, in terms of satisfying these requirements. Therefore, Information Security must become a central management and governance responsibility (Swindle & Conner, 2004). This means that the current way of addressing Information Security must change.

Information Security should not be viewed only as a technology issue. Information Security is a business and governance challenge that involves Risk Management, reporting and accountability on the part of executive leadership, including the BoD. The fragile state of Information Security demands that immediate steps be taken to ensure that data is not compromised and that information systems remain secure (Corporate Governance Task Force, 2004). External legislative and regulatory scrutiny places pressure on organizations to ensure their security functions are effective. Information Security

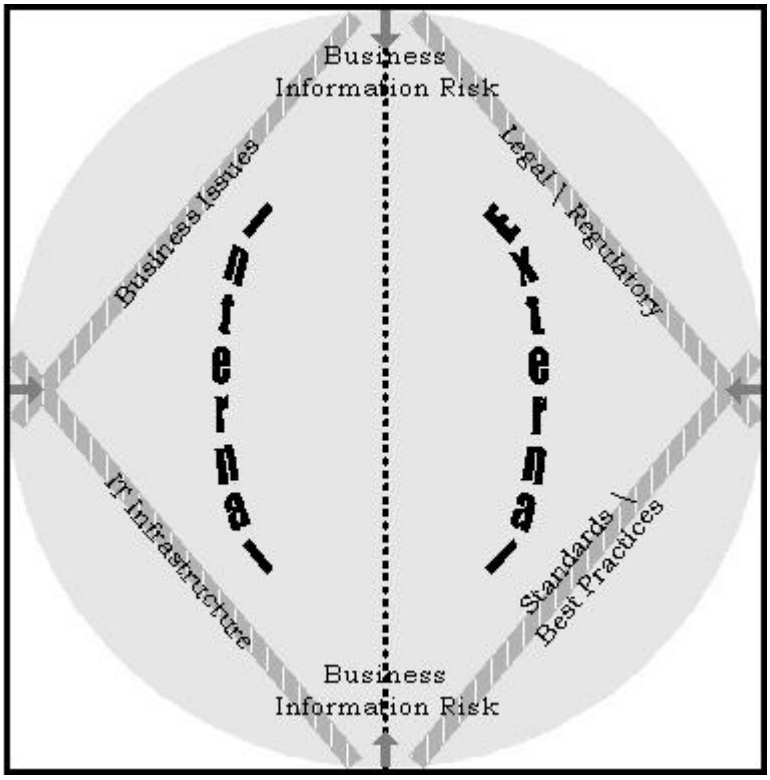


Figure 5.1: The internal and external requirements that contribute to an effective Information Security strategy.

is a strategic and legal issue (Birman, 2000). The Business Software Alliance (2004) states that "responsibility for the right level of security is a business decision based on risk assessment". The addressing of business information risk from a technology perspective alone is insufficient. Therefore, there is a definite need to elevate the importance of Information Security and integrate it into the overall Corporate Governance program (Corporate Governance Task Force, 2004). The Corporate Governance Task Force (2004) states that "the road to Information Security goes through Corporate Governance". This requires that organizations establish sound security direction by implementing Information Security as part of their internal controls and guiding principles which comprise their broader Corporate Governance program (Corporate Governance Task Force, 2004). Such internal controls and guiding principles dictate how an organization is directed and managed (Swindle & Conner, 2004). Therefore, integrating Information Security into the broader Corporate Governance program establishes it as a fundamen-

tal organizational business operation and imposes responsibility, in terms of Risk Management, reporting and executive accountability onto the BoD and Executive Management, including the CEO (Entrust, 2004a). The term Information Security Governance (ISG), describes Information Security as a component of the broader Corporate Governance responsibilities of an organization.

It is important that organizations consider an approach such as ISG to actively involve Executive Management, including the BoD and CEO, in the corporate Information Security function. This enables an organization to strategically align itself to be compliant with the legal stipulations that exist, while still achieving acceptable financial performance and reduced levels of business information risk. However, it is necessary to motivate this point by discussing why Information Security should be addressed at a governance level.

5.2.3 Why Information Security must be Addressed as a Governance Issue

A statement made by the Chinese General Sun Tzu more or less 2,400 years ago has relevance with relation to Information Security.

> *"If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle."*

Corporate executives and the BoD must be aware of what is expected of them in terms of Information Security should they hope to sustain successful and profitable business operations which produce adequate shareholder returns by reducing the potential of numerous business information risks. The BoD needs to understand their role with regard to the protection of corporate information assets.

The King Report (2001) on Corporate Governance clarifies why Information Security needs addressing as a Corporate Governance responsibility. Firstly, it is essential that the BoD understand that they are responsible

and accountable to the shareholders and, therefore, they must ensure that their organization produces business value and delivers a suitable return on shareholder investment (King Report, 2001). Sound Information Security efforts generate this return as Swindle and Conner (2004) motivate. The King Report (2001) states that Executive Management is responsible for ensuring that their organizations comply with applicable laws, regulations and codes of practice. This includes those laws and regulations and codes of best practice which ensure that Information Security is executed efficiently. It is in the best interest of the BoD and Executive Management to fulfill this responsibility as failure may result in legal action against them (Swindle & Conner, 2004). Furthermore, the King Report (2001) states that Executive Management should discover all significant areas of risk and certify that their computer systems and related technologies are capable of facilitating normal business operations. This includes identifying all aspects of business information risk, since such business information is a fundamental element of any organizational business process. This ensures that their information assets and business processes are fully and appropriately exploited, generating viable returns for the shareholders based on their investments (King Report, 2001).

Since information is such an important asset to any organization, it is the duty of the BoD to ensure that this resource is appropriately governed. Therefore, the BoD must understand several key considerations which will help them demonstrate support for Information Security and ensure that it is implemented effectively.

5.3 Effective Information Security: Considerations for the Board

The BoD must demonstrate due care and due diligence and be attentive in their corporate compliance efforts by considering legal and regulatory Information Security requirements to govern Information Security effectively. Furthermore, the issuing of the Corporate Information Security Policy (CISP) is important to align the organization with the objectives of the Bod for Information Security.

5.3.1 Due Care and Due Diligence

The term due diligence is defined as "the effort a party makes to observe its legal duty" to avoid harm to another party (Furnas, 2004). However, due diligence on its own is not enough. There needs to be consideration for due care as well. The term "due care", refers to the acknowledgment and execution of accepted best practices (Bergamo, 2005). Schoenberg (2005) states that "performing due diligence shows you where your risks lie, due care is exercising the requirements discovered under due diligence to protect or mitigate exposure from those risks".

It is important that Executive Management and the BoD exercise due care and due diligence in their organizations, ensuring the preservation of sensitive business information assets. Bergamo (2005) motivates the necessity of due care and due diligence by stating that the most sophisticated Information Security controls can be undermined through negligent actions. For example, it is possible that confidential business information, only meant for specific personnel, is stored on a company laptop which is lost or compromised (Bergamo, 2005). Another example involves computer users and their difficulty in remembering the numerous passwords they need to access information and work with particular programs. Consequently, such users may stick "post-it" notes on their workstations containing passwords and, thus, defeat the objective of technical access control mechanisms (Bergamo, 2005). The BoD and Executive Management need to ensure that such events do not take place, thereby, reducing the risks associated with these events.

Due care and due diligence are not only important for the business objectives of the organization for confidentiality, integrity and availability. Due care and due diligence enable an organization to demonstrate their compliance with the law which is not optional (Furnas, 2004). Non-compliance with laws and regulations can result in legal action against such organizations.

5.3.2 Laws and Regulations

Poor governance practices have resulted in greater external scrutiny over the way companies operate. The BoD is required to comply with a myriad of laws and regulations and must display appropriate due care and due diligence towards protecting business information. The consequences of non-compliance

with these regulations involve legal action such as large financial penalties and lengthy prison terms (Trillium Software, 2004). Regulatory intervention usually results in a tarnished corporate reputation which affects consumer and investor trust (Vericept Corporation, 2004). However, legal and regulatory requirements in terms of Information Security are important because of the ease of access to business information and services today. Entrust (2004a) motivates that "the very openness and accessibility that stimulated the adoption and growth of private networks and the Internet also threaten the privacy of individuals, the confidentiality of business information, and the accountability and integrity of transactions."

Information Security regulations are aimed at reminding executives and the BoD of their corporate accountability and responsibility. More importantly though, is the need to promote self governance, through an improved system of Corporate Governance with greater concern for Information Security due care and due diligence, as an alternative legislation (Entrust, 2004a). Executive Management and the BoD must ensure that they remain in complete control over an organization and understand the full scope of their duties. This ensures that organizational resources, including information, are not inappropriately exploited and the shareholders interests will be preserved.

There are various types of legal requirements that organizations are expected to comply with in terms of Information Security or face prosecution (Swindle & Conner, 2004). These include discipline specific and country specific statutes and laws. Some examples include the Sarbanes-Oxley Act (SOX), the Gramm-Leach-Bliley Act (GLBA) and the Health Insurance Portability and Accountability Act (HIPAA).

SOX applies to all public organizations that are exposed to US security laws and provides internal controls for financial reporting (Business Software Alliance, 2004). It aims to improve the accuracy of reporting mechanisms by demanding the establishment of proper reporting procedures and the assurance that these statements are current, comprehensive and precise (Trillium Software, 2004). ***GLBA*** is aimed at financial institutions and mandates the security of information relating to the customers of an organization (Business Software Alliance, 2004). The act delineates a formal framework for the implementation of managerial, technological and physical controls in this

regard (Vericept Corporation, 2004). ***HIPAA*** is targeted at health plans, health care clearing houses and health care providers and requires that patient health information in electronic form remains secure (Business Software Alliance, 2004). This requires the implementation of policies, procedures and technological controls allowing only authorized persons to access such information (Vericept Corporation, 2004).

An organization demonstrates its compliance with these various legal and regulatory requirements by specifying its goals and objectives for Information Security. These need to be communicated to the entire organization to ensure they meet compliance needs at all levels i.e. strategic, tactical and operational. Their communication is best achieved through the CISP.

5.3.3 Information Security Policy

Information Security must become part of the mission and goals of the organization. The BoD accomplishes this by ensuring there are appropriate security policies in place to avoid Information Security incidents (Bergamo, 2005). Bergamo (2005) states that senior executives "charged with maintaining the financial and material health of the organization, ... have a personal stake in setting the proper direction and security culture required to ensure that". Information Security policies play an important role in enabling Executive Management and the BoD in demonstrating their due care and due diligence for Information Security and compliance with the law.

Policies, generally, uphold the mission, vision, and business strategy of an organization (Whitman & Mattord, 2003c). They define actions that are acceptable and unacceptable in terms of organizational culture (Whitman & Mattord, 2003c). Similarly, an Information Security policy stipulates what is required to protect business information assets (Whitman & Mattord, 2003c). There are more detailed policies, that complement an Information Security policy, and focus on particular concerns such as the Internet, email, contingency planning and viruses (SecureSynergy SecurityScape, 2003). Executive Management and the BoD are required to consider three specific types of security policies namely, high-level or general security policies, issue-specific security policies and systems-specific security policies (Whitman & Mattord, 2003c).

The high-level security policy, also known as the CISP, guides the entire

security program of the organization (SecureSynergy SecurityScape, 2003). It expresses support for the mission, vision and direction of the organization and defines the high-level strategy to be followed to fulfill the Information Security function (Whitman & Mattord, 2003c). The CISP expresses the purpose of the Information Security function, allocates responsibility for its execution and approves corrective action against non-compliance (SecureSynergy SecurityScape, 2003). It directs the establishment, execution and administration of the entire Information Security function (Whitman & Mattord, 2003c). Issue-specific security policies provide details that state how various technologies and business processes should be utilized in an acceptable manner (Whitman & Mattord, 2003c). System-specific policies focus on specific issues more closely because they address one particular system and discuss these issues in detail (SecureSynergy SecurityScape, 2003).

It is important that the policy is not inconsistent with the law and should be able to stand up in a court of law if challenged (Whitman & Mattord, 2003c). All personnel in an organization should know about the Information Security policy, otherwise, it will be ineffective (SecureSynergy SecurityScape, 2003). The security policy should be distributed throughout the organization and be read, understood and agreed upon by all employees (Whitman & Mattord, 2003c). This helps Executive Management and the BoD to ensure that the organization fulfills its regulatory compliance objectives and acts lawfully and responsibly with regard to its daily business affairs. The meeting of such compliance objectives demonstrates Executive Management-level and board-level due diligence (Bergamo, 2005).

The demonstration of due diligence through the enforcement of policy provides several benefits. These include reducing individual and corporate liability and diminishing the potential for computer misuse (SecureSynergy SecurityScape, 2003). Effective security policies create business value and strategic advantage by improving the credibility of the organization and encouraging consumer and investor confidence (SecureSynergy SecurityScape, 2003). However, a security policy requires constant review and adjustment to remain effective as the business needs of the organization change (Whitman & Mattord, 2003c).

Policy is a central feature to the corporate Information Security function and demonstrates how the confidentiality, integrity and availability of busi-

ness information must be preserved in every respect. However, one of the problems noted about Information Security is that it is project driven and not necessarily policy driven (Citadel Security Software, Inc., 2005). Information Security should, nevertheless, be a business priority and a fundamental responsibility of the BoD. An optimum way to create a policy driven approach to Information Security is to incorporate it into the Corporate Governance objectives of the BoD through Information Security Governance.

5.4 Information Security Governance

Information Security Governance enables the BoD to become involved in the Information Security efforts of the organization. Therefore, there is a need to define Information Security Governance and emphasize its importance. It is important to differentiate between Information Security Governance and Information Security Management to illustrate how these separate but complementary functions are both necessary to ensure effective Information Security within an organization.

5.4.1 Information Security Governance Defined

The Corporate Governance Task Force (2004) states that "Corporate Governance consists of the set of policies and internal controls, by which organizations, irrespective of size or form, are directed and managed. Information Security Governance is a subset of organizations' overall governance program." Information Security Governance includes board-level involvement in terms of directing and controlling organizational Information Security efforts through policies and internal controls that govern the use of business information and the technologies that support its use.

Business information is very important. An organization has a competitive advantage over other companies, through having the right information at the right time (Gerber & von Solms, 2001). The BoD must ensure that its confidentiality, integrity and availability are maintained to protect the interests of the shareholders and generate business value. Information Security Governance enables the BoD to achieve this by focusing on Risk Management efforts, reporting and accountability with regard to its use (Corporate Gov-

ernance Task Force, 2004). This ensures that the risks affecting the security of business information are minimized to an acceptable level.

Information Security Governance is essential because it ensures there is board-level involvement in the organizational Information Security program, however, it is necessary to clarify why it is so important.

5.4.2 The Importance of Information Security Governance

Due to the ease of accessibility to information and business services through the Internet and other networks, information is exposed to three fundamental elements that create potential risks to its confidentiality, integrity and availability. These have been discussed and include people, business processes, various technologies and the Internet. Moreover, these elements are key features of Corporate Governance and require the attention of the BoD. Information Security Governance enables the BoD to devote their attention to people, processes and technology and brings accountability to each (Swindle & Conner, 2004).

The IT Governance Institute (2005e) highlights some additional factors that help demonstrate the importance of Information Security Governance. It states that:

- Risks and threats to information are real and can have a dramatic influence on the well-being of the organization;
- Effective Information Security efforts necessitate the need for co-ordination and integration throughout the organization to include all personnel;
- Investments in technology may be potentially significant and could possibly be misdirected;
- The institution and enforcement of rules and priorities is essential;
- There is a need to exhibit trust towards customers and business partners while conducting electronic transactions that involve the exchange of sensitive information;
- It is important to exhibit trust in the consistency of system security to all of the stakeholders of the organization;

- Breaches of Information Security may potentially be exposed to the general public;
- There is a possibility that the corporate reputation could suffer considerable damage due to ineffective Information Security.

Information Security Governance ultimately enables the BoD and Executive Management to ensure they have appropriate measures in place to sustain the organization, create business value and uphold shareholder expectations. It is important to not get confused between Information Security Governance and Information Security Management which was discussed in Chapter Four. The differences between the two should be examined.

5.4.3 The Difference between Information Security Management and Information Security Governance

It is essential to differentiate between Information Security Management and Information Security Governance to highlight the necessity of these functions in terms of securing business information assets. Information Security Governance and Information Security Management together form the unified process that constitutes the broader Information Security function of the organization. Each of these activities has a particular contribution to make in terms of Information Security and are thus both essential.

The BoD is responsible for effectively directing and controlling all aspects of the organization through sound governance efforts (King Report, 2001). This includes directing and controlling Information Security which becomes part of key organizational business operations (Entrust, 2004a). Information Security Governance is a board-level responsibility and is partly fulfilled with the development of the CISP. Its development demonstrates that Executive Management and the BoD supports the establishment and implementation of a comprehensive Information Security plan (Corporate Governance Task Force, 2004). Policy enables the BoD to direct the organization's Information Security program effectively.

The BoD controls security efforts through reporting mechanisms. It needs periodic reports from various organizational department heads, on the effectiveness of the overall Information Security program (Corporate Governance

Task Force, 2004). These reports enable the BoD to review the effectiveness of their Information Security direction and provide them with the necessary information to redirect such efforts as necessary. Various board-level committees make recommendations providing enough insight so the BoD can make accurate strategic decisions. It is important that Executive Management and the BoD are in control of Information Security efforts because, as Entrust (2004a) states, "like quality assurance, [Information Security] requires continuous, incremental improvement over time."

Information Security Management is concerned with how the stipulations of the BoD, expressed in the CISP, are implemented within an organization. Information Security Management involves the commitment of various department heads and managers in implementing the specifications of the CISP with the assistance of accepted codes of practice (Corporate Governance Task Force, 2004), such as ISO/IEC 17799. Activities such as identifying security controls and formulating procedures to counteract risks form the basis of Information Security Management. Once the security measures are implemented, business information risks and the usefulness of the selected security controls, is observed and reported back to Executive Management and the BoD (Corporate Governance Task Force, 2004). However, literature suggests that Information Security Management usually does not include personnel beyond the ranks of the CIO. Usually the CISO who is not in an executive level position is responsible for managing the Information Security program (Whitman & Mattord, 2003a). Information Security Management is a management responsibility and does not include board-level participation.

Figure 5.2 illustrates the relationship between Information Security Governance and Information Security Management.

Information Security Governance and Information Security Management are essential components of an effective strategy for dealing with business information risk at a management level and governance level. Information Security Management relies on effective governance efforts to be a success. This is because the effective governance of Information Security enables the setting of an accurate Information Security strategy which is implemented through Information Security Management. It is important that organizations are aware of the direction of know their Information Security efforts to protect their information assets effectively. It was previously stated that

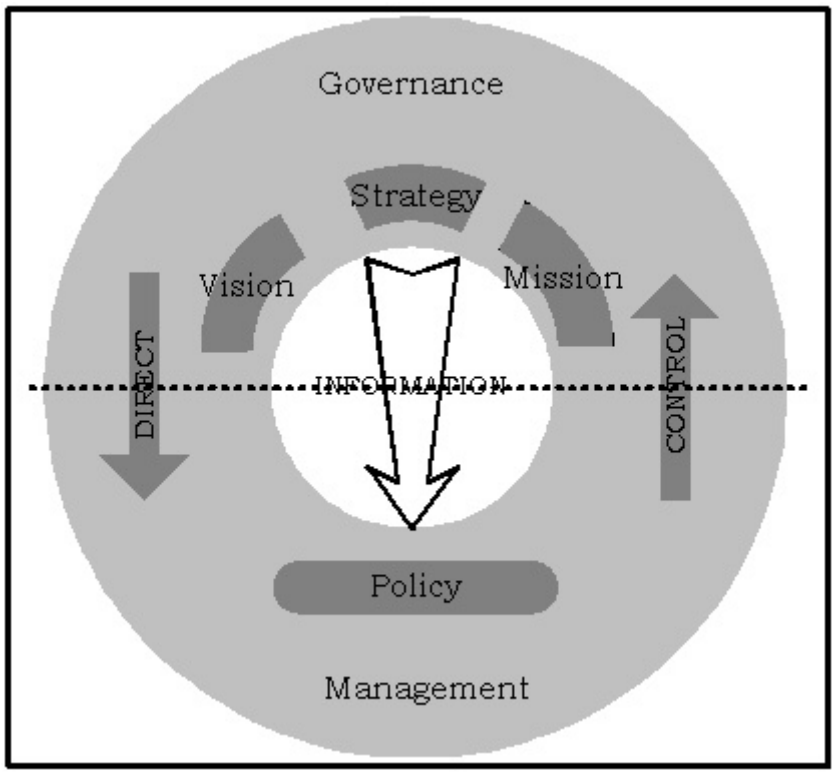


Figure 5.2: The Governance and Management Sides of Information Security

there is a lack of an adequate framework for Information Security Governance highlighting what must be accomplished and by whom (Business Software Alliance, 2004). It is necessary to propose an ISG framework to guide the BoD and Executive Management in their corporate Information Security endeavors.

5.5 A Framework for Information Security Governance

Information Security Governance is an important aspect of Corporate Governance and enables the BoD to become involved in the corporate Information Security function. However, the BoD needs clear direction in implementing ISG. A comprehensive framework will guide the BoD effectively in this regard. Therefore, the importance of an ISG framework will be motivated and it will be demonstrated how such a framework may be implemented. To support the proposed framework, the benefits of implementing ISG guided

by such a framework will be discussed.

5.5.1 The Need for an ISG Framework

Proper governance efforts require the methodical oversight and implementation of Information Security practices (Business Software Alliance, 2004). Therefore, proper governance operationalizes the Information Security function (Business Software Alliance, 2004). The BoD and Executive Management need guidance on how they should approach the corporate Information Security function from a governance perspective. There are many handbooks available that offer technical assistance and general Information Security principles in this regard (Business Software Alliance, 2004). Nonetheless, best practices, regardless of how strongly they are accepted, are by themselves insufficient and should be used with an Information Security Governance framework which promotes the successful execution of Information Security efforts (Business Software Alliance, 2004). A governance framework is essential because it provides a road map for the execution, assessment and enhancement of Information Security (Business Software Alliance, 2004). An organization that develops and implements an ISG framework can utilize it to express their Information Security goals and assess the Information Security function (Business Software Alliance, 2004). A good ISG framework achieves these objectives by satisfying certain criteria.

Entrust (2004a) points out that the Corporate Governance Task Force has outlined the following specific criteria that makes an ISG Framework effective:

- Demonstrate public-private cooperation for ISG i.e. it should be industry led and backed by the government;
- Distinguish ISG as a fundamental business/governance concern at the CEO and the Board level to demonstrate their personal and corporate accountability;
- Not industry or country specific, but, be generally applicable to all businesses whereas particular legislation such as HIPAA, GLBA industry specific;

- Be founded on industry standards like ISO/IEC 17799 and should be willingly put into practice through self-assessment;
- Encourage equilibrium between investment and business risk decision making i.e. begin with important areas of risk and proceed to others;
- Assist compliance with various regulations like Sarbanes-Oxley;

Once the BoD and Executive Management have understood the importance of ISG and what it entails to create a good ISG framework, the next step is to take the necessary actions to implement the framework.

5.5.2 How to Implement Information Security Governance

Effective Information Security Governance efforts are essential. A proper framework enables the BoD determine what steps their organization should take to define their Information Security direction. This supports the implementation of an accurate system of internal control. A good ISG framework makes the BoD aware of both internal and external security requirements and guidelines that have been discussed. These requirements together with the guidance of industry best practices and well-regarded security standards, like ISO/IEC 17799 (2005), help the BoD establish the foundation for an effective approach to Information Security. In a sense, such requirements represent directives that the BoD and Executive Management need to consider to holistically address all aspects of information risk. The examination of these will allow the BoD to outline the orgaizational vision, mission and Information Security strategy successfully. These are communicated to the organization through the CISP. Once the BoD has expressed their support of Information Security through the policy, management implements Information Security in the organization to fulfill its stipulations. Security is monitored on an ongoing basis and the BoD made aware of the Information Security efforts through management reports. This allows the BoD to continue to direct and control corporate Information Security efforts accurately by making the necessary adjustments to the Information Security strategy to keep it as effective as possible and minimize business information risk.

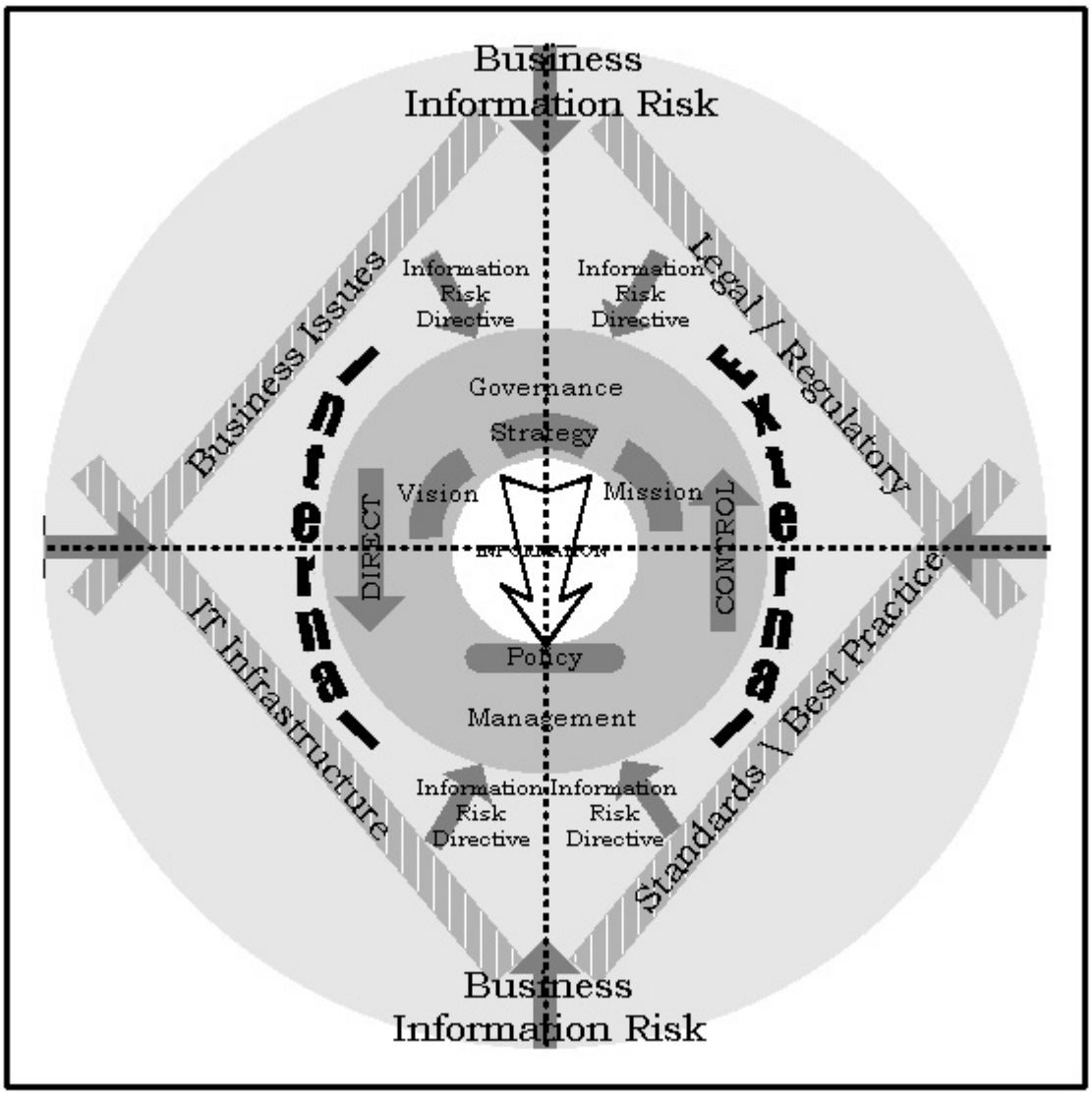


Figure 5.3: An Information Security Governance Framework

Figure 5.3 illustrates a framework for Information Security Governance, which draws attention to the major security requirements and how they all contribute guiding the BoD in terms of accurate Information Security decision making and the implementation of an effective Information Security Management strategy.

It is important to have a proper framework like the one proposed above to govern and manage Information Security effectively. The application of such a framework will bring accountability to people, process and technology elements through effective Risk Management and reporting mechanisms. Such accountability is introduced by indicating who should be responsible

for what, making it possible to allocate particular Information Security tasks and responsibilities (Business Software Alliance, 2004).

5.5.3 Information Security Roles, Tasks and Responsibilities

An important function of Information Security Governance involves denoting the roles of various individuals in the organization to effectively implement the ISG framework and ensure its success. There is a need to identify the key role players and discuss their Information Security tasks and responsibilities in more detail.

The Role of the Board of Directors

The fundamental role of the BoD is to oversee the interests of the shareholders by directing and controlling the organization effectively and ensuring that all resources are responsibly exploited. Therefore, with regard to information as a business resource, the BoD must understand its significance and the significance of protecting it through directing and controlling Information Security efforts successfully (Corporate Governance Task Force, 2004). Additionally, the BoD must support the establishment and implementation of a robust Information Security program and receive management reports on the utility and effectiveness of the program (Corporate Governance Task Force, 2004). This enables the BoD to ensure that their security efforts remain effective and current.

The Role of Board Committees

Board Committees facilitate the BoD in executing their duties efficiently and demonstrate that their responsibilities are being appropriately accomplished (King Report, 2001). There are various board-level committees that offer assistance to the BoD in terms of their responsibility for Information Security. These committees include: the IT Oversight Committee, the Audit Committee and the Risk Management Committee.

The role of the IT Oversight Committee is to advise the BoD on an appropriate IT strategy for the organization (IT Governance Institute, 2004). The

IT Oversight Committee ensures that organizational IT strategy supports Information Security, since IT is closely linked to this resource (IT Governance Institute, 2004). The IT Oversight Committee will be discussed subsequent chapters. The Audit Committee is responsible for conducting performance reviews of the system of internal control and reviews legal and regulatory compliance efforts (King Report, 2001), including that of Information Security. The Risk Management Committee advises the BoD regarding corporate accountability and management, reporting and assurance related risks (King Report, 2001). Its terms of reference include technology, operational, disaster recovery, and compliance and control risks (King Report, 2001).

The Role of the Chief Executive Officer

The Chief Executive Officer is responsible for overseeing the entire Information Security program (Corporate Governance Task Force, 2004). The CEO oversees compliance efforts and enforces accountability for such efforts (Corporate Governance Task Force, 2004). Furthermore, the CEO also reports compliance issues to the BoD, highlighting the level of acceptable risk, weaknesses in current Information Security practices and plans to strengthen those practices (Corporate Governance Task Force, 2004). The CEO allocates responsibility, accountability and authority for various security functions to the right organizational personnel and appoints someone as the senior Information Security officer (Corporate Governance Task Force, 2004).

The Role of the Chief Information Officer

The Chief Information Officer makes recommendations to the CEO on the strategic planning efforts affecting the administration of organizational information resources (Whitman & Mattord, 2003a). The CIO converts the strategic plans of the organization into strategic plans for information and information systems (Whitman & Mattord, 2003a). The CIO collaborates with other non-executive managers developing plans of a tactical and operational nature for the management of information and information systems. These efforts entail setting the policies and procedures for Information Security (Corporate Governance Task Force, 2004).

The Role of the Chief Information Security Officer

The Chief Information Security Officer is responsible for the overall Information Security Management function (Whitman & Mattord, 2003a). Some of the CISO's responsibilities include collaborating with the CIO on strategic Information Security plans, establishing tactical plans and collaborating with security managers on operational security plans (Whitman & Mattord, 2003a). The CISO plans the Information Security budget and acts as the representative for all security personnel (Whitman & Mattord, 2003a).

The Role of Data Owners (The Business Unit Leaders)

One of the responsibilities of the business unit leaders include implementing the specifications of the more detailed security policies and procedures (Corporate Governance Task Force, 2004). They audit the effectiveness of various security procedures and communicate the security policies and procedures to other subordinate personnel through staff training initiatives (Corporate Governance Task Force, 2004). They enforce compliance with the security policies (Corporate Governance Task Force, 2004).

These security roles and responsibilities span the entire organization, involving personnel in both management and governance positions, including the BoD. Information Security that is implemented correctly with the right roles assigned to the right individuals through effective Information Security Governance efforts produces several benefits.

5.5.4 The Benefits of Information Security Governance

Information Security Governance is a complex issue requiring the commitment of everyone in an organization to fulfill their role in protecting organizational business information assets. Information Security Governance, if executed effectively, is of value to organizations in ways that exceed the mere observance of lawful conduct (Swindle & Conner, 2004). Effective Information Security Governance results in enhanced internal security practices and controls and the promotion of self-governance as an alternative to legislation (Entrust, 2004a). Sound ISG efforts have the potential to reduce auditing and insurance costs and differentiate the organization from industry competitors through an ongoing process of self-improvement (Entrust, Inc., 2004).

ISG is a useful function for increasing overall productivity and lowering costs by delivering strategic alignment with broad organizational strategies and risk appetites (IT Governance Institute, 2005e). This produces value for stakeholders, including governments and legislative authorities (Swindle & Conner, 2004), by improving Risk Management efforts and enabling better performance measurements to provide assurance that information-related risks are under control (IT Governance Institute, 2005e).

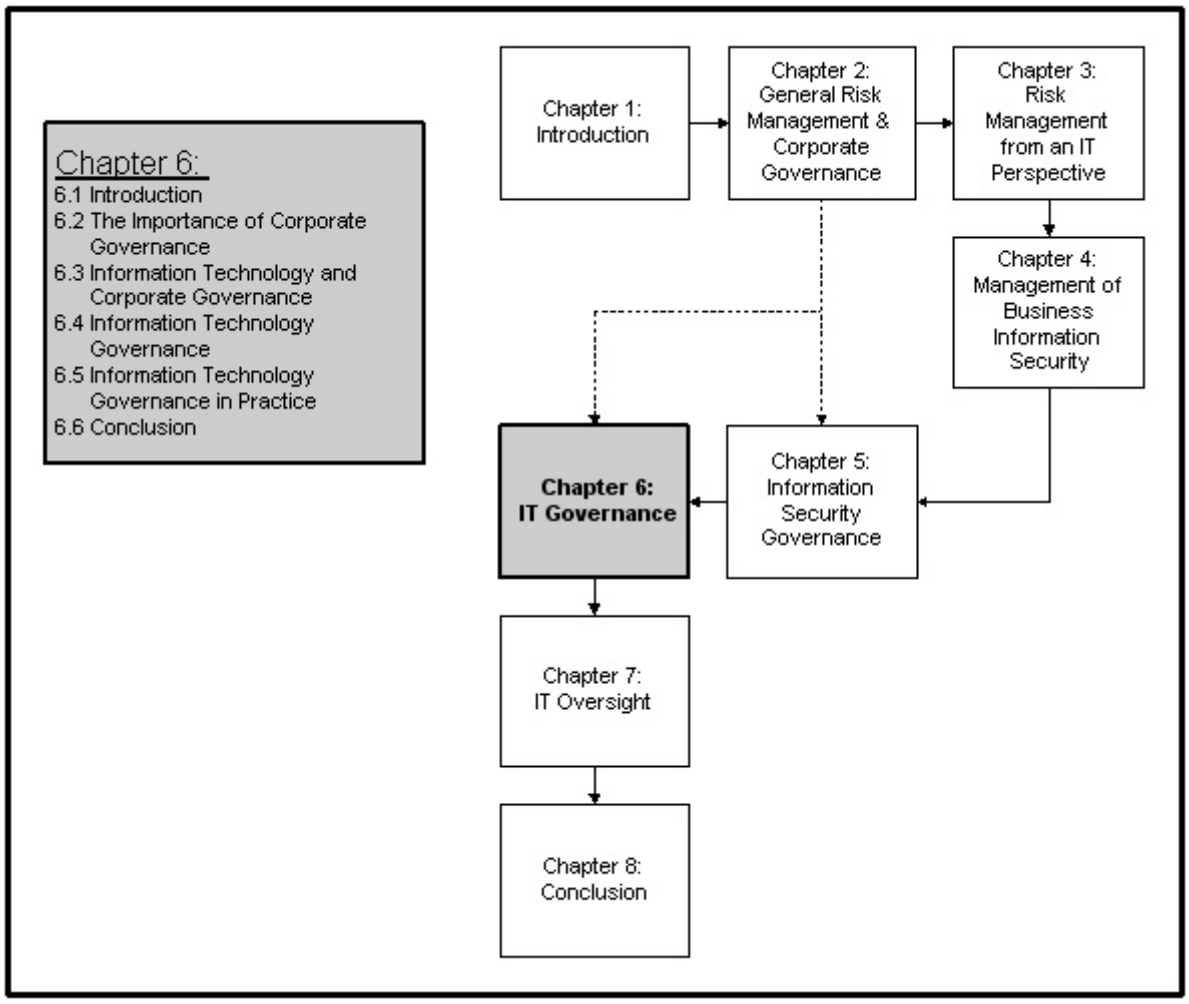
5.6 Conclusion

Information Security is becoming a major issue of concern, to both the private and public sectors, including governments around the world (Corporate Governance Task Force, 2004). The Corporate Governance Task Force (2004) recommends that effective governance frameworks should exist. Entrust (2004a) motivates that the acceptance and implementation of an ISG framework is an important action in securing business information. This is achieved through the protection of information systems, whilst acting in accordance with legislation and improving the efficiency of business operations. Information Security Governance enables an organization to demonstrate due care and due diligence by fulfilling the internal and external security requirements for protecting business information assets effectively. It caters for the full scope of organizational information risks. Therefore, it is important that Executive Management, including the BoD and CEO, adopt an ISG framework, such as the one presented above. This will help guide the implementation of an effective Information Security Governance strategy and address all aspects of business information risk. However, as dependence on IT to facilitate business operations and deliver timely and accurate information increases, IT's criticality becomes a fundamental business concern. Therefore, effective Information Security Governance requires that IT be addressed at board level. This ensures that the implementation and utilization of technology resources is appropriately governed through effective IT decision making and risk management efforts. This ensures that technology-related information risks are brought to the attention of the BoD, enabling their ISG efforts to be effective in addressing every aspect of business information risk. For this reason, IT governance must become a key function of Corporate

Governance and responsibility of the BoD.

Chapter 6

Information Technology Governance



6.1 Introduction

Information Technology Governance should be a core responsibility of the BoD and Executive Management. Many organizations rely heavily on IT making it nearly impossible to continue with normal business operations or deliver timely and accurate business information without it. Therefore, IT-related risks need to be understood by the BoD and Executive Management and brought under control. This is to ensure that Information Security Governance is effective in addressing all aspects of information-related risks and that value is drawn from the organization-wide use of IT. This chapter aims to motivate the importance of IT Governance as a core responsibility of the BoD for value delivery and the management of IT-related risks, including those that affect information. The need for IT Governance is motivated by discussing the importance of comprehensive Corporate Governance practices by illustrating some general governance failures like Enron Corp. and WorldCom Inc., which occurred because of board-level ignorance. The criticality of IT is discussed and various issues that inhibit its effective use in an organization. The responsibilities of the BoD, in terms of IT, are examined to demonstrate what needs to be done to ensure its effectiveness in an organization. The best way for the BoD to express their commitment is to ensure that IT is effective and IT-related risks are mitigate through IT Governance, which is discussed in detail to highlight its importance and relationship to Corporate Governance. Additionally, the scope of IT Governance is discussed and how it may be implemented using accepted IT Governance frameworks such as COBIT. The benefits of implementing IT Governance based on the recommendations of an accepted IT Governance framework such as COBIT are also discussed.

6.2 The Importance of Corporate Governance

Effective Corporate Governance should be a priority in any organization because it is the mechanism through which the BoD directs and controls all organizational affairs preserving shareholder interests. This demonstrates the need for good Corporate Governance which will be discussed in detail. Additionally, some Corporate Governance failures will be discussed to highlight

the consequences associated with poor governance practices.

6.2.1 The Need for Good Governance

Today, well-informed and confident stakeholders are becoming more concerned about the reliable supervision of their interests (IT Governance Institute, 2003). Numerous governance principles and standards have been drafted to guide the accomplishment of the general governance endeavors of the organization (IT Governance Institute, 2003). Additionally, various laws and regulations introduce board-level responsibilities and call for the demonstration of board-level due diligence through compliance (IT Governance Institute, 2003). This signifies that compliance forms a significant part of the overall Corporate Governance function.

Compliance is characterized as the state of being in agreement with the appropriate government, industry and various additional regulatory authorities and their prerequisites (Jennings, 2004). It concentrates on defending the rights of the stakeholders, which include employees, investors, customers and business partners (Jennings, 2004). Compliance is directly linked to Corporate Governance because if it signifies requirements and expectations placed on an organization by external bodies, then Corporate Governance is the reaction of the organization to fulfill such requirements (Jennings, 2004). Therefore, Corporate Governance is essential to ensure that organizations have aligned themselves with various legal, regulatory and other requirements that external parties expect of them.

The Report of the Committee on the Financial Aspects of Corporate Governance i.e. The Cadbury Report, has attracted attention to the subject of Corporate Governance (IT Governance Institute, 2003). The Cadbury Report includes more specific requirements relating to financial reporting and auditing, but, demonstrates concepts generally applicable in the broader sense of Corporate Governance (IT Governance Institute, 2003). The Cadbury Report suggests transparency, integrity and accountability are required to develop standards of corporate behavior, reinforce controls over corporations and their public accountability while still maintaining the fundamental essence of the organization (IT Governance Institute, 2003). It categorizes a variety of board-level Corporate Governance tasks. Some of these include:

- Establishing strategic objectives;
- Demonstrating sound leadership;
- Overseeing management;
- Providing statements to the organization's shareholders on their stewardship (IT Governance Institute, 2003).

Corporate Governance is essential to provide assurance that the recommendations stipulated by documents such as The Cadbury Report are fulfilled appropriately and successfully.

In Chapter Two it was mentioned that a survey carried out by McKinsey and Company showed that investors are aware of the significance of good governance. This is demonstrated through the fact that they are prepared to purchase shares at potentially more than 20 percent premium in an organization that exhibits good Corporate Governance practices (IT Governance Institute, 2003).

It is important that all organizations attempt to implement Corporate Governance effectively because this attracts investment and sustains organizational growth and also avoids the risks of non-compliance. Poor governance practices did, recently, lead to the downfall of several prominent organizations in the USA, leaving them bankrupt and with severely damaged corporate reputations.

6.2.2 Corporate Governance Failures

Some prominent examples of Corporate Governance failures include those of Enron Corp. and WorldCom Inc. Enron Corporation, a Houston-based energy trading company, filed for corporate bankruptcy in late 2001, becoming the largest bankruptcy case in United States history, having in excess of $62 billion in corporate assets (Vinten, 2002). The reason for the collapse of Enron Corp. was due to inaccurate accounting practices and a weak system of internal control. Jeffrey Skilling, the CEO of Enron Corp., admitted to not understanding the off-balance-sheet accounting and, therefore, left it to the accountants (Nolan, 2004), with little further concern. A similar scenario played out at WorldCom Inc., a US telecommunications company, where it was found that the Audit Committee of the BoD was lacking in financial

experts (Nolan, 2004). Furthermore, the Audit Committee charter of WorldCom Inc. claimed that they could not be held accountable for their financial statements due to this lack of financial expertise (Nolan, 2004).

Poor governance practices, unmistakably, caused these disasters. The BoD in each of these organizations did not retain full and effective control over all corporate affairs or consider characteristics such as transparency, integrity and accountability as recommended by The Cadbury Report. Effective Corporate Governance is essential to sustain an organization. According to both Changepoint Corporation (2004) and Nolan (2004), there is a salient issue that may soon become a Corporate Governance concern, potentially leading to situations similar to those that occurred at Enron or WorldCom, if it is continuously ignored. This issue is concerned with the use of information technology within an organization.

Changepoint Corporation (2004) motivates that directors are guided by the fact that they are the custodians of shareholder capital, of which a significant amount is invested in IT. A recent survey by the National Association of Corporate Directors (NACD) reveals that the most critical interests of the BoD are CEO relationships and their succession, organization performance and valuation, accountability systems, strategic planning and risk (Changepoint Corporation, 2004). Each of these concerns is linked with IT excluding the matter of CEO succession (Changepoint Corporation, 2004). It is important to examine the role of IT within the broader Corporate Governance framework and as a responsibility of the BoD.

6.3 Information Technology and Corporate Governance

Information Technology can have a major impact on an organization. It is necessary to discuss its criticality in business and demonstrate some factors that inhibit its appropriate exploitation within an organization. It is also important to discuss the responsibility of the BoD in terms of appropriately exploiting this resource to produce acceptable business value and reduce all forms of IT-related risks including those that affect business information.

6.3.1 The Criticality of Information Technology

Today, IT is a major facilitator of organizational business activities. IT spending has escalated and figures attest that approximately 55 percent of company capital investments are IT based (Nolan, 2004). The efficient and innovative application of IT in business has the ability to revolutionize organizations and plays a role in increasing and maintaining shareholder value (IT Governance Institute, 2005a). Nevertheless, greater complexity, speed, interconnectivity and globalization indicates that IT has the potential to incur great costs and significant risks (IT Governance Institute, 2005b). Considerations such as cost, risk and opportunity make IT strategic to organizational development and cause it to be fundamental to the continued existence of the organization (IT Governance Institute, 2005b).

Organizations must manage and exploit IT-related risks and opportunities effectively to achieve success. Therefore, IT requires considerable board-level guidance in terms of Risk Management and governance endeavors (Changepoint Corporation, 2004). The general prerequisite to express high-quality Corporate Governance to organizational shareholders and consumers is the driving force for improved enterprise Risk Management (IT Governance Institute, 2005d). The risks faced by most organizations are quite diverse and do not only include those of a financial nature (IT Governance Institute, 2005d). Regulatory authorities are worried about operational and systematic risks. The critical aspects of such broad risk areas include the risks associated with IT and information security (IT Governance Institute, 2005d).

There is a growing perception that IT is becoming a critical success factor for financial growth and corporate prosperity in the 21st century (IT Governance Institute, 2005b). Most organizations depend on IT to attain a competitive edge in business and it is crucial that they pay the same amount of attention to IT issues as they do to matters of finance and general Corporate Governance (IT Governance Institute, 2005b). The IT Governance Institute (2003) motivates that “IT is fundamental for managing enterprise resources, dealing with suppliers and customers, and enabling increasingly global and dematerialized transactions. IT is also important for recording and disseminating business knowledge”. Additionally, the IT Governance Institute (2005b) emphasizes three primary reasons why IT is critical to an

organization. These are:

- IT directly adds to the business value of an organization;
- IT is an indispensable tool enabling the accomplishment of business goals;
- IT involves significant investments and associated risks.

Despite the apparent criticality of IT to achieve business success in the 21st century, there are numerous factors that inhibit the appropriate exploitation of IT in organizations. It is important to address these inhibiting factors to give a clear indication about what organizations can do to overcome these and enjoy the benefits of the effective and proper use of IT which serves to strengthen information security.

6.3.2 Factors Inhibiting the Effective and Proper Use of IT in an Organization

Organizations have spent vast amounts of money on corporate IT investments, however, the alignment of IT strategy with the business objectives still seems to be a concern today (Luftman, Papp, & Brier, 1999). Luftman et al. (1999) illustrates several factors that inhibit such alignment. Firstly, there appears not be a close relationship between the business and its IT resources. Additionally, IT appears not to prioritize effectively and does not seem to deliver on its commitments. Furthermore, IT seems to not understand the business Luftman et al. (1999).

The IT Governance Institute (2005c) provides some reasoning why such inhibitors exist within organizations. While sound efforts are made to achieve the alignment of business and IT, many organizations do not have proper governance structures in place to facilitate such alignment (IT Governance Institute, 2005c). Furthermore, IT, which plays a fundamental role in enabling an organization to achieve business success, requires extensive and insightful governance efforts (Scottsdale Institute, 2001). However, sufficient governance efforts over the corporate IT function are scant because of the perception that IT is more an operational issue to be addressed at a management level (Scottsdale Institute, 2001). Corporate boards do not have the

interest or the skill to deal with technology matters regardless of the fact that IT involves substantial investments and significant amounts of risk (Scottsdale Institute, 2001). Such situations demonstrate that IT management does not have sufficient leadership (Luftman et al., 1999).

These inhibitors widen the gap between the expectations of IT and reality which, in most cases do not correspond, according to the IT Governance Institute (2003). The IT Governance Institute (2003) states that this creates a situation where the BoD is faced with:

- Significant company losses, a tarnished corporate reputation and a competitive stance that is ineffective;
- Inability to acquire or gauge the returns from investments in IT;
- Inability of IT to deliver on the promises of innovation and organizational gains;
- Ineffective or outdated technology resources;
- Failure to exploit the latest technologies;
- Missed deadlines and exceeded budgets.

Such poor direction and control of the corporate IT function has great potential to place information assets at risk. The significance and worth of business information assets in most organizations are underrated (IT Governance Institute, 2005b). The IT Governance Institute (2005b) demonstrates that research conducted by the Brookings Institute revealed that merely 15 percent of the business value of an organization comes from tangible assets whereas 85 percent is derived from intangible assets and mainly constitutes business information. It is extremely important to have effective governance efforts in place to oversee the corporate IT function and mitigate IT-related information risks (IT Governance Institute, 2005b). Consequently, IT should become a fundamental board-level concern, therefore, the BoD must become aware of their responsibilities in terms of overseeing IT as a critical organizational resource.

6.3.3 The Board's Responsibility for IT

It is important that the BoD and Executive Management understand the position and influence of IT in an organization, outline the operational constrains of IT personnel, gauge the ability of IT to perform, become aware of IT-related risks and acquire assurance (IT Governance Institute, 2005b). This enables the BoD and Executive Management to give better IT direction and control enabling them to:

- Exploit the ability of IT to facilitate new business models and evolving business practices;
- Obtain an equilibrium between the escalating costs of IT and the increasing worth of information assets to acquire suitable gains from technology investments;
- Deal with risks relating to business transactions performed in a networked business environment and risks relating to reliance on parties outside of the immediate control of the organization;
- Deal with issues of business continuity relating to IT as a result of a growing dependence on information and various technologies throughout the organization;
- Sustain the ability of IT to establish and preserve data which is critical for organizational support and development;
- Circumvent IT-related failures which constantly influence organizational business value and corporate reputation (IT Governance Institute, 2003).

IT risk assessment is a core function in all planning efforts within the organization and should concentrate on the infrastructure related vulnerabilities of IT, the degree of exposure of intangible assets like information to various security and operational risks and the risks that may cause IT projects to fail (IT Governance Institute, 2005b).

Boards of directors should consider IT in terms of its cost, risks and its opportunities (IT Governance Institute, 2005b). They should determine if IT is producing returns for the organization and achieving its objectives (IT

Governance Institute, 2005b). It is important for the BoD to set the appropriate strategy to ensure that IT is aligned with the overall business strategy and support organizational business objectives, which include maintaining the security of the information assets.

The IT Governance Institute (2005c) states that effective governance over the accomplishment of IT business alignment requires proactive leadership and the commitment of the BoD and the CEO. In this regard, the BoD must ensure that the IT strategy, which must be aligned with the business strategy, actually delivers against this strategy (IT Governance Institute, 2005c). The BoD must guide IT strategy effectively to ensure that technology investments are evenly spread across the critical systems of the organization that support it, transform it and produce organizational growth (IT Governance Institute, 2005c). It is important that the BoD make well-informed decisions regarding where to apply and prioritize for the use of IT assets in the organization (IT Governance Institute, 2005c). Lastly, the BoD must ensure that suitable IT and other business assets are obtained to allow IT to meet its potential (IT Governance Institute, 2005c).

It is important that IT-related issues are properly addressed at board level within an organization due to the criticality of IT in business today. However, it is no simple task for the BoD to maintain control over the corporate IT function because this requires a significant amount of investment in terms of time, necessary skills and other resources. A formalized governance framework enables the BoD to give effective IT direction and control. Thus, IT Governance, which is rapidly becoming an essential element of Corporate Governance, facilitates the BoD with their accountability for corporate IT affairs.

6.4 Information Technology Governance

Information Technology Governance is extremely important to ensure that corporate IT assets are appropriately exploited. It is important to define IT Governance by discussing it in detail. Furthermore, the relationship between IT Governance and Corporate Governance is highlighted and its importance as part of the overall Corporate Governance function.

6.4.1 IT Governance Defined

The directing and controlling of the use of new technologies, which includes consideration for IT, expands the mission of the BoD with regard to outlining corporate strategy and ensuring business objectives are achieved, risks are dealt with and corporate assets are utilized appropriately (Scottsdale Institute, 2001). The extensive exploitation of technology has caused a major reliance on IT that requires particular attention to be paid to IT Governance (Scottsdale Institute, 2001). It must ensure that corporate IT resources maintain and expand business strategies and objectives (Scottsdale Institute, 2001).

The IT Governance Institute (2003) states that "IT Governance consists of the leadership and organizational structures and processes that ensure that the organization's IT sustains and extends the organization's strategy and objectives". Additionally, Van Grembergen (2002) motivates that "IT Governance is the organizational capacity exercised by the Board, executive management and IT management to control the formulation and implementation of IT strategy and in this way ensure the fusion of business and IT".

Peterson (2003) demonstrates that although these two definitions are somewhat different, their focus is essentially the same i.e. attaining the alignment between IT and business. Additionally, Peterson (2003) points out that the definition of Van Grembergen suggests that IT management is included in the IT Governance function. However, it is important to note IT Governance and IT management are distinct from one another as IT management is concerned with the successful provision of IT services and products and the everyday administration of the IT function (Peterson, 2003). In contrast, IT Governance has a wider focus and devotes attention to executing and converting IT to deliver on the current and prospective needs of the organization and its consumers (Peterson, 2003).

Essentially, IT Governance is about the policies and procedures that determine how an organization will direct and control the use of its technology resources, ensuring these resources facilitate the realization of its business goals successfully. Jennings (2004) motivates that IT Governance is a continuous process, requiring ongoing review and adjustment and involves several concepts, including Risk Management, security, business continuity, change management, and regulatory compliance. It is important to note that IT

Governance does indeed encompass these activities but from a technology perspective and not one that would necessarily address all aspects of information risks. Consideration for these various concepts, enables an organization to utilize its IT resources in an appropriate manner and with maximum efficiency, thereby contributing significantly towards service enablement and business value creation (Webb & Robertson, 2004). Hence, this demonstrates how the IT Governance function is able to support "the alignment of business and IT", as Jennings (2004) motivates, to achieve competitive advantage and economic success.

Information Technology Governance is a useful tool for directing and controlling the technology aspects of an organization. Technology has become a major business enabler, serving to increase company profits and shareholder value. This places pressure on the BoD since, according to the King Report (2001), it is responsible for ensuring that their technology resources are adequate to properly carry out their business activities. Hence, the BoD needs to understand their role in IT Governance and its impact on the overall Corporate Governance function. Therefore, it is important to discuss the relationship between IT Governance and Corporate Governance.

6.4.2 The Relationship Between IT Governance and Corporate Governance

The IT Governance Institute (2004) claims that IT Governance is not an isolated discipline. IT Governance must become a fundamental element of Corporate Governance, and requires board-level attention to ensure that IT-related risks and the return on IT investment are adequate in terms of the business needs of the organization (IT Governance Institute, 2004). Ron Exler, a Robert Francis Group analyst, states that Corporate Governance and IT Governance are "intimately intertwined". Exler (2003) further states that "increased scrutiny on Corporate Governance directly and indirectly affects IT and the direction IT Governance will take ... in an era where technology is critical to business, Corporate Governance is incomplete without adequate IT Governance."

Information Technology Governance generally entails employing broad Corporate Governance principles in a strategic way to direct and control

the IT component of the organization (IT Governance Institute, 2005b). IT Governance Institute (2005b) states that IT Governance should call attention to:

- The capability of IT to exploit and have an effect on intangible assets such as information, knowledge and trust;
- The linking of IT and the business strategies of the organization;
- The appraisal and endorsement of investments in IT;
- The assertion of transparency regarding IT-related risk;
- IT performance assessment.

The BoD must understand that their accountability and responsibility in terms of Corporate Governance extends into IT through a system of IT Governance. Proper Corporate Governance efforts, therefore, include all attempts to direct and control the use of information technology in an organization effectively (Webb & Robertson, 2004). This means that such efforts involve strategic planning for IT to support the business goals, as well as the formulation of policies, procedures and management structures required to attain such goals (Jennings, 2004). Corporate executives and the BoD need to recognize that their endorsement and participation in this regard is critical, especially in terms of communicating the accepted IT strategy, which is now an integral part of the overall business strategy of an organization (Jennings, 2004).

The importance of IT Governance will be discussed to demonstrate to the BoD why there is a need to ensure that IT Governance becomes a fundamental component of the organization's broader Corporate Governance function.

6.4.3 Why is Information Technology Governance Important?

Stakeholder values are central to the governance functions of the following:

- Setting corporate strategy

- Creating business value
- Dealing with risks and assessing performance
- Guiding the organization and its IT strategy (IT Governance Institute, 2003).

Stakeholders anticipate that the organization should continue to exist and be developed through new business models, which can only be accomplished through acceptable IT Governance endeavors (IT Governance Institute, 2003).

Information technology is a major facilitator regarding the storage, processing and transmission of business information resources, which are vital to produce competitive advantage and increased business value to increase stakeholder returns. The use of this information and its privacy are strictly governed by a myriad of laws and regulatory compliance mandates passed in the wake of various Corporate Governance failures like that of Enron Corp. and WorldCom Inc. Consequently, regulatory compliance efforts are elevated to a top priority on the corporate executive agenda, with information security as a central element of concern.

Information technology is intrinsic and pervasive within most organizations, which requires governance to specific notice of IT, assessing how dependent the organization is on IT and how vital IT is for carrying out corporate strategy (IT Governance Institute, 2003). As previously stated, Entrust (2004a) motivates that technologies such as the Internet and other private networks have the potential to greatly "threaten the privacy of individuals, the confidentiality of information and the accountability and integrity of transactions.". This emphasizes that the use of IT needs to be strictly governed. Hence, good IT Governance has become a crucial part of successful compliance efforts (Jennings, 2004).

The Scottsdale Institute (2001) states that effective IT Governance will protect the interests of the shareholders and ensure that IT-related risks are properly analyzed and understood. Additionally, it will enable better direction and control over the IT investments of the organization, its opportunities, benefits and risks (Scottsdale Institute, 2001). It ensures that IT is aligned with the overall business strategy and demonstrates recognition that IT has a crucial contribution to make (Scottsdale Institute, 2001). Effective

IT Governance makes it possible to sustain the existing business functions and enables planning for the future (Scottsdale Institute, 2001).

The necessity of IT Governance has been motivated and the next step is to take the required actions to implement IT Governance. Therefore, it is necessary to demonstrate how IT Governance can be put into practice.

6.5 Information Technology Governance in Practice

The practice of effective IT Governance requires the understanding of it covers as far as the resources of the orgization are concerned. Furthermore, how IT Governance is implemented will be discussed with relation to particular IT Governance frameworks that exist, such as COBIT for example. Additionally, some of the benefits of implementing IT Governance based on accepted frameworks like COBIT will be discussed.

6.5.1 What Does Information Technology Governance Cover?

The IT Governance Institute (2003) states that IT Governance is primarily concerned with two main issues, these are its ability to produce business value and the management of all IT-related risks. The former is achieved through the strategic alignment of IT with the business goals of the organization while the latter is achieved through the establishment of accountability in the organization (IT Governance Institute, 2003). Each of these issues require the allocation of sufficient resources and must be monitored to ensure that the organization utilizes IT with maximum efficiency and offers stakeholder value (IT Governance Institute, 2003). IT Governance covers five main focus areas to achieve this:

- The delivery of IT value;
- IT Risk Management;
- Strategic alignment of IT and business;
- Resource management;

- The appraisal of IT's ability to deliver i.e. performance measurement (IT Governance Institute, 2003).

The IT Governance Institute (2005a) discusses each of these five focus areas in more detail:

Strategic Alignment is concerned with ensuring there is a link between the business and IT plans of the organization. These plans can include the delineation, preservation and support of IT value proposition and the alignment of IT functions with broader corporate business functions (IT Governance Institute, 2005a).

Value Delivery focuses on carrying out the value proposition, ensuring that IT produces its potential benefits against business strategy, by directing attention to the reduction of costs and demonstrating its inherent value (IT Governance Institute, 2005a).

Resource Management is concerned with acquiring the most favorable investments in, and the effective management of, crucial IT resources. These include people, business processes, the IT infrastructure, software and business information. Critical concerns involve the enhancement of knowledge and the infrastructure (IT Governance Institute, 2005a).

Risk Management necessitates the need for Executive Management and the BoD to become aware of IT-related risks and the risk appetite of the organization, demonstrate transparency with regards to considerable organizational risks and the establishment and delegation of responsibilities for Risk Management in the organization (IT Governance Institute, 2005a).

Performance Measurement records and observes the implementation of IT strategy within the organization, the completion of IT projects, the utilization of resources, how well the processes execute and the services are delivered (IT Governance Institute, 2005a).

Information Technology Governance needs to be implemented effectively for each of these focus areas to be covered adequately. However, effective IT Governance is a challenge, therefore, it needs to be implemented based on the recommendations and guidelines of accepted IT Governance frameworks such as COBIT which will be discussed in detail.

6.5.2 How to Implement Information Technology Governance

Information Technology Governance is a continuous process which begins with strategy setting and alignment in the organization (IT Governance Institute, 2003). The implementation of IT Governance commences and the key deliverables at this stage include the value assured by the strategy and the mitigation of all IT-related risks (IT Governance Institute, 2003). It is fundamental that the strategy be effectively monitored and measured on a regular basis, reported on and any necessary actions taken to enhance the strategy if needed (IT Governance Institute, 2003).

The implementation a good system of IT Governance is not a simple task. There are many things that influence the environment in which most organizations function. These include:

- The values of the stakeholders;
- The organization's own mission, visions and values;
- The principles and culture of the organization and the community it serves;
- Various relevant laws, regulations and policies;
- Industry best practices (IT Governance Institute, 2003).

Fortunately, today, there exist several IT Governance frameworks that help to guide an organization and the BoD in these endeavors. One such framework is the internationally accepted Control Objectives for Information and related Technology (COBIT).

The Control Objectives for Information and related Technology was compiled by the Information Systems Audit and Control Association and the IT Governance Institute. It is an IT assessment tool that is utilized to evaluate the ability of IT to deliver on its promise of value and aims to provide the BoD with sufficient information to keep them informed about IT-related issues in their organization (Scottsdale Institute, 2001). The COBIT framework emphasizes the alignment of organizational business goals with various

IT control processes (Webb & Robertson, 2004). COBIT consists of 34 high-level control objectives, each for a particular IT process, which are categorized into four primary domains of best practice for IT performance (COBIT, 2000). These are, planning and organization, acquisition and implementation, delivery and support, and monitoring (COBIT, 2000).

The Control Objectives for Information and related Technology is based on the idea that IT is critical to deliver the business information required by the organization for it to accomplish its corporate goals (Scottsdale Institute, 2001). COBIT helps demonstrate which of the characteristics of information i.e. confidentiality, integrity, availability, effectiveness, efficiency, reliability and compliance and what IT resources i.e. people, software, technology, facilities and data are essential for organizational business objectives to be adequately assisted by the various IT functions (Scottsdale Institute, 2001). COBIT offers a sufficient system of control for an IT environment as it caters for all considerations in terms of information and organizational technology resources that facilitate its use (COBIT, 2000).

An organization will deliver an IT strategy that supports information security and increase business success, through sound IT Governance (Webb & Robertson, 2004). Such a strategy could include, for example, as Webb and Robertson (2004) put it, automating the value chain by implementing systems for Enterprise Resource Planning (ERP), Supply Chain Management (SCM) and Customer Relationship Management (CRM), which is currently imperative to sustain a competitive edge in business.

The underlying premise of COBIT is business orientation (Scottsdale Institute, 2001). It is designed to be implemented not only by users and auditors, but also by Executive Management and business process owners who require broader direction (Scottsdale Institute, 2001). The Scottsdale Institute (2001) states that "increasingly, business practice involves the full empowerment of business process owners so they have total responsibility for all aspects of the business process".

The effective implementation of IT Governance guided by the recommendations of an internationally accepted framework such as COBIT can produce significant benefits for an organization.

6.5.3 The Benefits of Information Technology Governance

Proper governance frameworks, that have been customized to satisfy organizational business strategy, enable the effective apportionment of resources, the monitoring of performance and management of IT-related risks by enabling sound decision making and the provision of value (Webb & Robertson, 2004).

MIT's Sloan School of Management determined that enterprises "with superior IT Governance have more than 25 percent higher profit than firms with poor governance given the same strategic objectives" (Weill & Woodham, 2002). These days it is clear that business priorities such as enhancing organizational productivity, driving down costs, and boosting the value of investments in IT show that IT Governance can produce benefits (Webb & Robertson, 2004). The effective implementation of IT Governance provides several enablers that contribute toward IT business alignment. Luftman et al. (1999) highlights these enablers which include:

- The backing of IT by Executive Management and the BoD;
- The development of a corporate strategy which includes consideration for IT;
- The business affairs of the organization being understood by its IT component;
- Cooperation and collaboration resulting in the linking of business and IT. Webb and Robertson (2004) states that "discipline in the interaction of corporate officers, business leaders, and the IT organization, breaks down barriers, focuses stakeholders on business strategy, and promotes quality decision making that results in value creation and well-managed IT";
- The effective prioritization of organizational IT projects;
- The expression of leadership through effective IT direction and control.

These benefits corroborate that effective IT Governance can have a dramatic and positive effect on an organization. It enables a better managed

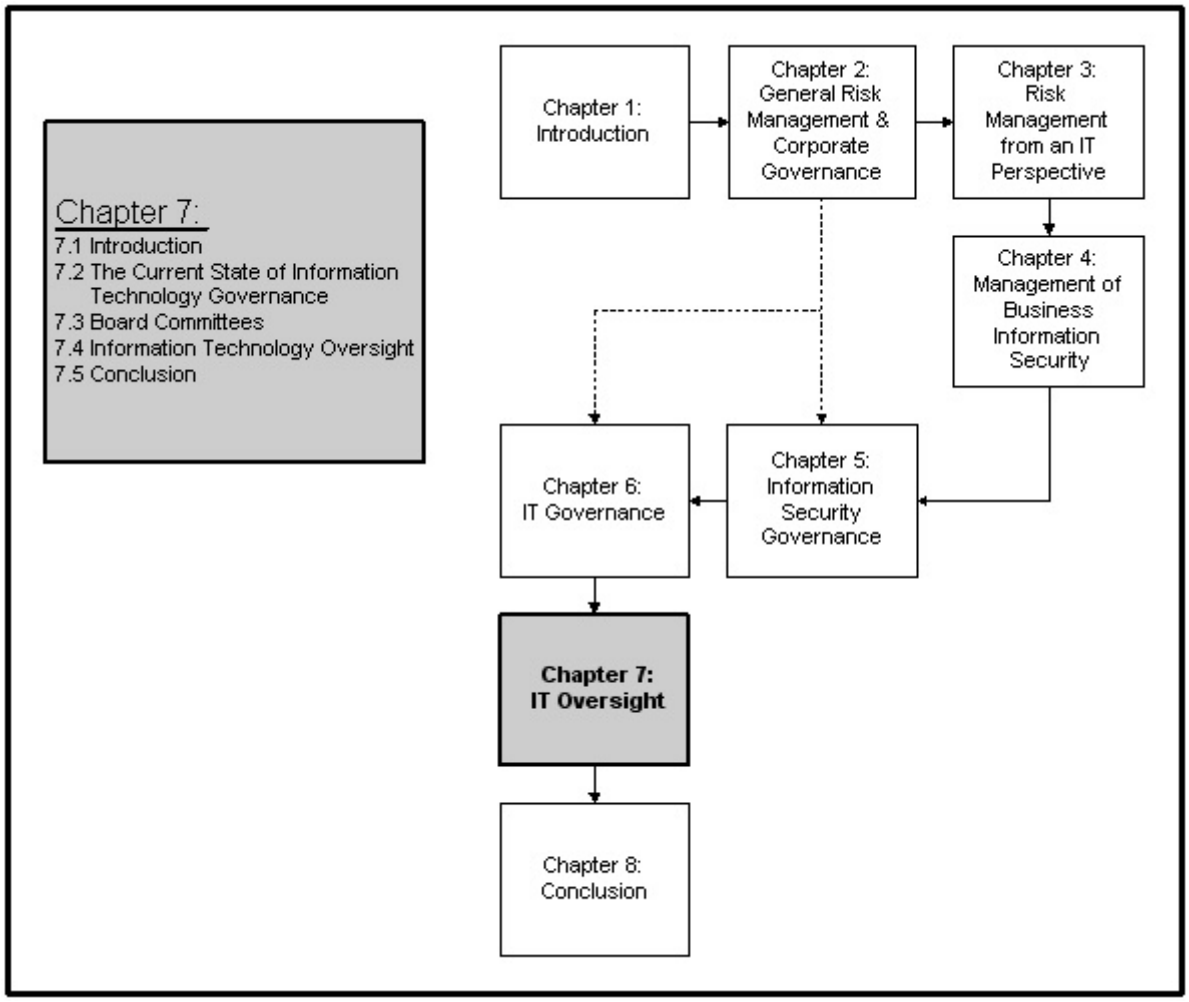
and more secure business environment which provides those organizations who accept this challenge with a strategic advantage over their competitors and increase returns and satisfy their shareholder expectations.

6.6 Conclusion

Information Technology Governance should become a fundamental component of Corporate Governance for the BoD and Executive Management to retain full and effective control over the business affairs of the organization, preventing disasters like that of Enron Corp. and WorldCom Inc. IT has a critical role to play in facilitating key business operations and the usage of business information. Therefore, efficient IT Governance practices will reduce IT-related risks, including those that affect information, and ensure that organizational business operations continue to function normally. Effective IT Governance requires that the BoD make well-informed decisions with regard to IT. However, although they may be guided by IT Governance frameworks such as COBIT, the Scottsdale Institute (2001) states that they lack the skills and insight necessary to strategically direct and control IT effectively. Usually, board-level committees are responsible for informing the BoD on specialized matters, like the Audit Committee on the financial aspects of the organization. The next chapter motivates the institution of an IT Oversight Committee to help advise the BoD in terms of IT Governance, IT-related risks and other strategic IT issues, and thereby bring about a stronger system of internal control and an enhanced approach to Corporate Governance.

Chapter 7

IT Oversight



7.1 Introduction

The critical role that IT currently plays in most organizations means that executives need to understand how to apply an IT strategy effectively to maximize the benefits from their technology investments and reduce business information risk. IT Governance is a significant challenge because the BoD and Executive Management appear to lack the necessary skills to drive the IT strategy effectively. This chapter promotes the necessity of the IT Oversight Committee (ITOC) to enable the BoD and Executive Management to make accurate decisions in terms of IT strategy and IT Risk Management. This ensures the organization is able to implement an effective approach to Information Security Governance, based on the proposed ISG framework in Chapter Five, that addresses all aspects of business information risks including IT-related ones. This will demonstrate that the primary objective of this study, which was to develop an ISG framework and promote the significance of IT oversight enabling all aspects of business information risk to be governed, has been met.

This chapter promotes the necessity of the IT Oversight Committee by discussing the current state of IT Governance, looking at various IT Governance failures and who is responsible for board-level IT guidance. Various board-level committees are discussed, highlighting the extent of their advisory duties to the BoD and whether or not these are sufficient to provide board-level IT guidance. The IT Oversight Committee is discussed to demonstrate its function with relation to IT decision making at board-level and in IT Risk Management which plays a fundamental role in Information Security Governance.

7.2 The Current State of Information Technology Governance

Information Technology Governance can be a significant challenge. This is evident from numerous IT Governance failures which are discussed. These failures appear to arise from a lack of IT decision making skills at a Corporate Governance level. Therefore, the question of who is responsible for facilitating the BoD in terms of accurate IT decision making should be addressed.

7.2.1 Some Information Technology Governance Failures

Poor IT Governance practices, spurred on by weak board-level guidance, produces significant amounts of loss and places information assets at risk. These situations arise from improper planning efforts (Girard, 2002). Additionally, bad investment decisions which can lead to the complete restructuring of organizational IT strategy.

In 2001, IT-related losses were more than $1.5 billion from four major companies alone. During this time, the Internet division of Disney suffered a $878 million loss when it was forced to shut down its Go.com portal because it was unable to remain competitive against its industry rivals, AOL and Yahoo (Girard, 2002). Additionally, Kmart wrote-off $130 million due to supply chain hardware and software investments that failed to meet their expectations (Changepoint Corporation, 2004). Furthermore, Gateway, a computer manufacturing company, lost $143 million due to the scrapping of various IT projects that no longer supported their corporate IT strategy, which was in the process of being restructured due to a $2.2 billion drop in sales and dwindling profit margins (Girard, 2002). Another IT Governance failure in 2001 involved Nike. Their $400 million loss was due to a bad investment in supply chain management software which failed to support its objectives (Changepoint Corporation, 2004). Nike lacked sufficient IT expertise on this project and held little regard for the fact that a significant amount of IT resources had already been allocated to other ERP and CRM ventures currently under way (Changepoint Corporation, 2004).

It appears that corporate boards appear to be making ill-advised decisions in terms of IT and are, therefore, having difficulty in implementing good systems of IT Governance. This gives the impression that such boards lack adequate board-level IT guidance and are, therefore, inappropriately overseeing shareholders interests. Should situations like this continue to emerge, even more Corporate Governance disasters may transpire because weak board-level guidance, in relation to IT, will prevent the BoD from retaining complete control over an organization. This serves to weaken the overall Corporate Governance endeavors of the organization, including Information Security and places business information at risk. A situation like

this may lead to low public confidence and result in greater external scrutiny and the enforcement of more regulation. It is necessary to examine who is responsible for advising the BoD in terms of IT Governance and what can be done to improve the current situation to resolve this issue.

7.2.2 Who is Responsible for Board-Level Information Technology Guidance?

The role of the BoD, in terms of IT Governance, is strategic direction and control. It is the responsibility of the CIO to ensure that IT Governance is properly executed within an organization (Changepoint Corporation, 2004). Therefore, the BoD looks solely to the CIO for assurance that the corporate IT strategy supports the underlying business objectives of the organization (Changepoint Corporation, 2004). The CIO appears to play a major role in demonstrating the effectiveness of the implemented IT strategy to the BoD. The BoD is expected to direct and control organizational technology efforts and make adjustments as necessary to ensure value delivery, business alignment and the mitigation of IT-related risks. However, one question remains, who, on the BoD, has the knowledge and experience ensure that proper business decisions, in terms of IT, are made on behalf of the shareholders?

In many organizations the responsibility for board-level IT guidance belongs to the Audit Committee (Changepoint Corporation, 2004). However, because of recent IT Governance failures, it is necessary to ascertain whether any currently active board committees, including the Audit Committee, have the expertise required to advise the BoD on IT matters.

7.3 Board Committees

Board committees contribute significantly to the overall Corporate Governance endeavors of an organization. It is important to explore, in detail, the role that such committees play to gain a clearer picture of the scope of their functions and indicate their competence in terms of IT direction and control.

7.3.1 The Importance of Board Committees

The King Report (2001) states that any organization should have, at least, an active Audit Committee and a Remuneration Committee. Another committee recommended by the King Report (2001) is the Risk Management Committee. The duties of these committees should be examined to ascertain whether they are capable of providing practical insight into strategic technology based decisions given the issue of IT Governance and board-level guidance.

7.3.2 The Audit Committee

The Audit Committee has the responsibility of conducting an in-depth review of all audit-related issues within an organization (Cadbury Report, 1992). Both the King Report (2001) and the Cadbury Report (1992) highlight some more specific responsibilities of the Audit Committee.

One of these responsibilities is to conduct a performance review of the system of internal control of an organization (King Report, 2001). The Audit Committee is required to review the workings of the Audit Department, including the nature and scope of the audit process, highlighting any areas of concern (Cadbury Report, 1992). It is important that they evaluate the correctness of the financial statements prior to these being presented to the BoD (Cadbury Report, 1992).The Audit Committee is responsible for reviewing legal and regulatory compliance efforts, including the adherence to the rules and codes of conduct of the organization (King Report, 2001).

These are some of the responsibilities of the Audit Committee. These duties indicate that the make up of such a committee requires significant financial and auditing expertise.

7.3.3 Other Board Committees

The Remuneration Committee is responsible for dealing with all human resource related issues within an organization. One of its responsibilities includes reviewing and suggesting to the BoD executive and non-executive director compensation (Cadbury Report, 1992).

Risk and Risk Management are important considerations within an organization. Organizations may establish a formalized board-level committee to

deal with organizational risk. This committee is known as the Risk Management Committee. It is responsible for the quality, integrity and reliability of organizational Risk Management endeavors (King Report, 2001). It assists the BoD in terms of corporate accountability and the risks related to management, assurance and reporting (King Report, 2001). Its terms of reference include technology risk, disaster recovery risk, operational risk, and compliance and control risks (King Report, 2001). Some of the duties of the Risk Management Committee according to the King Report (2001) include:

- Evaluate and appraise the integrity of the systems of risk control in an organization and ensure that the policies and strategies that address risk are suitably administered;
- Specify the characteristics, position, responsibility and influence of the organizational Risk Management operation and establish the extent of Risk Management activities;
- Monitor external progress in terms of the execution of enterprise accountability and the reporting of related risk, together with any potential effects;
- Provide independent and unbiased supervision and evaluation of the information made available by management on enterprise accountability and associated risk, while considering management and Audit Committee reports to the BoD on financial, organizational and strategic risk.

The Audit Committee, the Remuneration Committee and the Risk Management Committee fulfill important roles within an organization. However, what can be said about these committees and their duties regarding their support of the BoD in terms of dealing with IT-related issues?

7.3.4 Are These Committees Sufficient?

It should be apparent from examining the duties of the Audit Committee, the Remuneration Committee and the Risk Management Committee that they fulfill highly specialized functions for the BoD. These committees require expert skills and the input of executives and other individuals to accomplish

their assigned roles efficiently. Previously, it has been the duty of the Audit Committee to review the proposed IT investments of the organization (Changepoint Corporation, 2004). However, based on the skills required by such a committee to address audit and accounting issues, the Audit Committee employs individuals who possess financial, accounting and auditing expertise. These individuals may not necessarily have an in-depth understanding of IT, which is required to guide the BoD in strategic IT decisions (Changepoint Corporation, 2004). In the literature on Corporate Governance, such as the King Report (2001), there is no direct reference that the Risk Management Committee have IT experts serving on it. Such committees, lacking in the necessary skills to support the BoD in terms of IT, have great potential to ill-advise it, possibly leading to financial losses similar to those of Disney, Nike and the others mentioned earlier. Therefore, Nolan (2004) asserts that "the next big thing in Corporate Governance ... is the board level IT oversight committee". Such a committee would be similar to the Audit and Compensation / Remuneration Committees (Nolan, 2004). Additionally, it would have the necessary skills to enable accurate IT decision making. Hence, IT oversight serves to strengthen the overall IT Governance program of the organization.

7.4 Information Technology Oversight

There is a need to highlight the importance of the IT Oversight Committee to demonstrate its proposed structure and functions and differentiate it from other organizational committees that address IT-related issues to clarify the usefulness of IT oversight as a strategic business function.

7.4.1 The Importance of the Information Technology Oversight Committee

A major portion of shareholder capital is invested in IT and the BoD is expected to ensure that these investments serve the interests of the shareholders by providing them with adequate returns (Changepoint Corporation, 2004). However, as previously stated, IT receives little attention at board level (Nolan, 2004). This situation leaves room for poor IT decision making,

potentially leading to the loss of capital, low investor confidence or financial ruin. The implementation of an IT Oversight Committee appears to be a practical mechanism for providing the necessary skills and insight to support technology based decision making and addressing strategic IT-related issues. Nolan (2004) asserts that organizations implementing such committees will be "better positioned to avoid disasters, they'll also be better positioned to size up the business value of emerging technologies ... and find opportunities to use IT to differentiate themselves, reduce costs and create strategic value". The IT Governance Institute (2004) maintains that such a committee is the best means for introducing proper governance over IT, by providing the BoD with the right information to support their IT Governance objectives. The Scottsdale Institute (2001) states that "setting up a working group, [such as an IT Oversight Committee], that does not hold voting authority or decision-making power can lessen a CEO's concerns about diluting authority. At the same time, such an advisory body can offer technical advice while helping to educate the board". Furthermore, an IT Oversight Committee facilitates the BoD in achieving better legal and regulatory compliance (IT Governance Institute, 2004). Additionally it helps to avoid major Corporate Governance risks similar to those that brought down Enron Corp. and WorldCom Inc.

Information Technology oversight helps to improve the overall Corporate Governance strategy of the organization, since it enables the BoD to demonstrate the characteristics of good Corporate Governance and aids them in fulfilling their Corporate Governance responsibilities better. Some of these responsibilities include providing comprehensive strategic direction to the organization, maintaining complete and successful control over the affairs of the organization and identifying and watching over important areas of organizational risk (King Report, 2001). The functions and composition of a proposed IT Oversight Committee are discussed to facilitate the BoD in properly fulfilling these responsibilities.

7.4.2 Information Technology Oversight Committee Functions and Composition

The IT Governance Institute (2004) states that the goal of the IT Oversight Committee is to ensure that IT is a standard topic on the corporate agenda

of the BoD and that it is dealt with in an organized way. The underlying responsibility of the IT Oversight Committee is to ensure that there is a constant channel of communication between Executive Management, the BoD and those who work in the IT department of the organization (Nolan, 2004). Nolan (2004) suggests that this communication should address five key topics. These are the management of information and IT resources, IT strategy, regulatory and compliance issues, service levels and the management of IT-related risks. Each of these topics depend on one another and are complimentary, therefore, the neglect of one can result in the failure to consider another appropriately (IT Governance Institute, 2004). There are ten questions that Nolan (2004) states an IT Oversight Committee should ask with regard to these five key topics. These are:

1. Does the organization receive acceptable returns from investments in business information resources?

2. Does the organization have the necessary IT resources to take full advantage of its intellectual property?

3. Does the organization have the necessary management functions in place to reduce the risk of technology obsolescence?

4. Does the organization have a sufficient amount of security measures to guard its corporate information assets?

5. Does the organization boast the necessary management practices to ensure it operates 24/7 service levels?

6. Are there functions implemented to ensure the detection and implementation of IT strategic opportunities are taken full advantage of?

7. Does the organization have the necessary functions in place to ensure any IT failure will not have a significantly negative impact?

8. Does the organization employ benchmarking as a regular function to uphold a competitive cost structure?

9. Does the organization have the necessary practices in effect to reduce the possibility of expensive lawsuits?

10. Does the organization have the necessary procedures implemented to ensure there are no IT-based surprises to Executive Management?

An important point to consider is that the IT Oversight Committee fulfills purely an advisory role to the BoD on issues such as these, therefore, it has no say in any final decisions reached by the BoD (IT Governance Institute, 2004). Mellon Financial Corporation (2004) highlights some specific advisory duties of the IT Oversight Committee in their Technology Committee Charter. These include advising the BoD and Executive Management on the development and execution of strategic plans that exploit existing and new technology effectively, assessing the viability of proposed new technology investments and overseeing IT performance and advising the BoD on the value delivery of IT in supporting the overall strategic business objectives (Mellon Financial Corporation, 2004). The IT oversight committee should collaborate with other board-level committees, particularly with the Audit Committee regarding important technology-related risks and the Compensation / Remuneration Committee with regard to performance measurement, to fulfill these duties appropriately (IT Governance Institute, 2004).

The members of the IT Oversight Committee should be chosen carefully, based on skills and experience that demonstrate their understanding of the impact of IT on the business, should its functioning be of value to an organization (IT Governance Institute, 2004). These members should include both board and non-board representation (IT Governance Institute, 2004). Nolan (2004) suggests that members should consist of CIOs, IT consultants and general managers, possibly appointed from outside the organization. These executives should be experienced in directing IT-related operations and recognize the strategic opportunities that IT presents (Nolan, 2004). The IT Oversight Committee must be aware of what is happening both internally and externally to the organization enabling them to provide the BoD with useful information on which to base strategic IT decisions (Nolan, 2004).

Currently, many organizations implement IT Steering Committees to help address numerous IT-related issues. Some may, as a result, scrutinize the necessity of creating another committee at board level i.e. the IT Oversight Committee. The functions of these two committees are compared to substantiate the validity of an IT Oversight Committee.

7.4.3 The Difference Between the Information Technology Oversight Committee and an Information Technology Steering Committee

One of the primary differences between an IT Steering Committee and the IT Oversight Committee is that an IT Steering Committee consists mainly of business unit leaders and department heads and does not normally include members such as the CEO or CFO (Hoffman, 2004). An IT Steering Committee does not operate at board level but at management level. The IT Oversight Committee, however, does include board-level participation, the same as any other sub-committee of the BoD and operates at board level. These differences demonstrate that the functions of the IT Oversight Committee and an IT Steering Committee are dissimilar. The aim of the IT Oversight Committee is to make recommendations to the BoD regarding an appropriate IT strategy for the organization (IT Governance Institute, 2004). From this point one or more IT Steering Committees assists Executive Management in implementing the IT strategy decided upon by the BoD (IT Governance Institute, 2004). Some typical duties of an IT Steering Committee include overseeing significant IT projects and handling IT priorities and the allocation of IT resources (IT Governance Institute, 2004).

The IT Oversight Committee helps the BoD set an appropriate strategy for organizational IT Governance endeavors, whereas, one or more IT Steering Committees aim to implement this strategy to realize the vision of the BoD in terms of IT Governance.

7.5 Conclusion

The provision of clear insight and advice in terms of IT strategy contributes towards an improved system of internal control that better supports the overall Corporate Governance objectives of the organization as well as information security. However, there is a possibility that the discussions of the IT Oversight Committee may become too detailed or technical and it is necessary to emphasize that its focus should remain on IT oversight and strategic planning (Nolan, 2004). There appears to be some debate about the membership of the IT Oversight Committee. Previous findings are based

on current literature, but, IT oversight is still a new concept which is subject to review and adjustment. However, corporate BoDs who undertake the challenge of IT oversight demonstrate that they understand the scope of their corporate accountability and responsibility and are proactive in their leadership duties and understand that since IT plays a major role it is necessary to govern its use effectively to reduce risks to corporate information assets. Although, none of the prominent Corporate Governance manuals or approaches dictate the existence of an IT Oversight Committee, several sources have promoted its employment. Therefore, it can be motivated that an IT Oversight Committee is an absolute necessity when IT plays a major role in business, according to the arguments presented in this chapter.

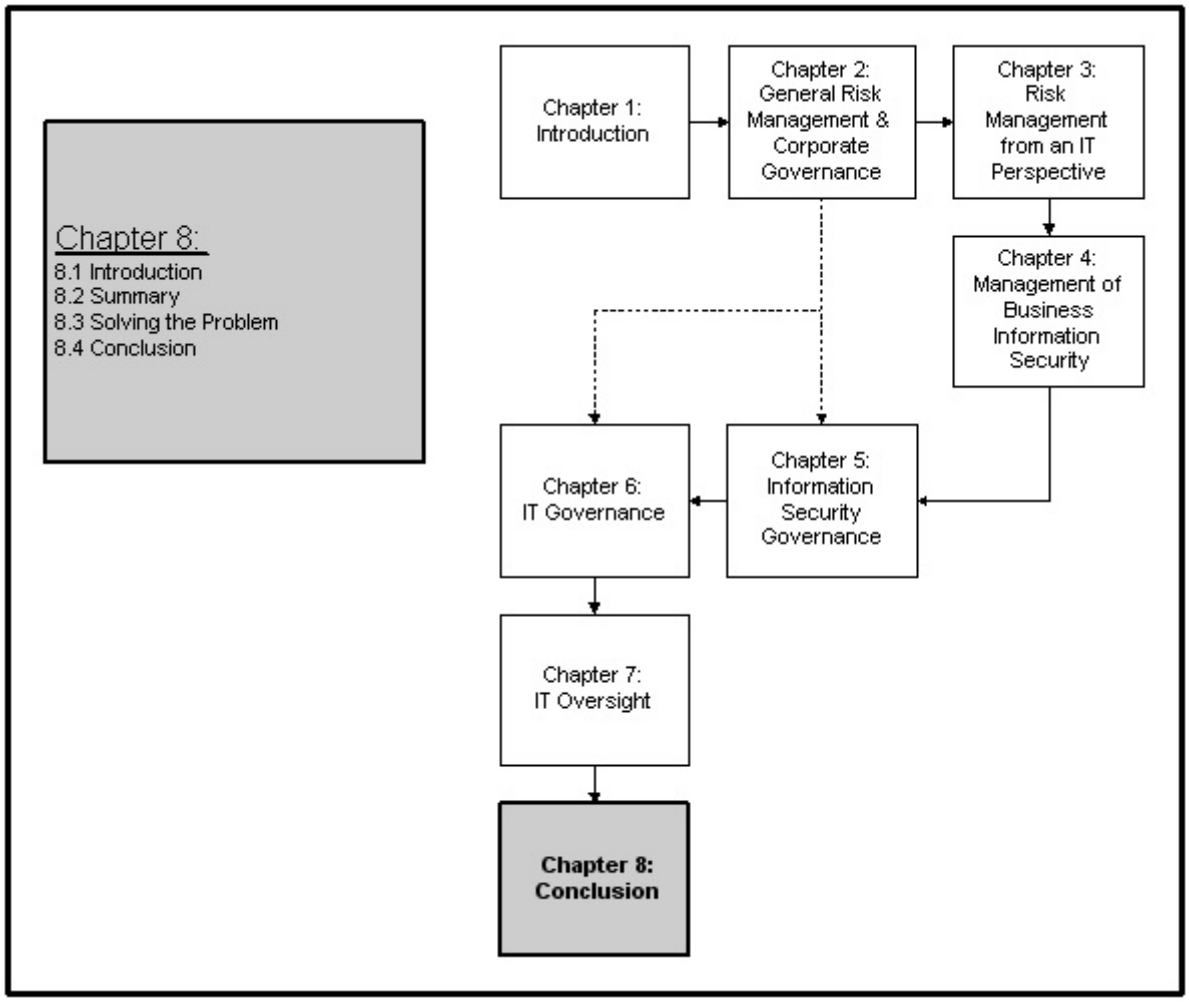
These arguments demonstrate the accomplishment of the primary objective of the study. This objective involved the development of an ISG framework and the promotion of the significance of IT oversight enabling all aspects of business information risk to be governed effectively. This ensures the effective alignment of IT with business and that information risks, including IT-related ones, are understood by the BoD and mitigated effectively through ISG and IT oversight. The achievement of the primary objective marks the resolution of the primary research question and emphasizes the importance of Information Security as a Corporate Governance responsibility.

Part IV

Conclusion

Chapter 8

Conclusion



8.1 Introduction

Information Security is an important organizational function. This dissertation aims to emphasize the importance of Information Security as a Corporate Governance responsibility. Several key topics were discussed through the various chapters of the dissertation to achieve this. Some of these topics include Corporate Governance, Risk Management and the impact of IT on modern organizations. Greater dependence on IT has led organizations to be exposed to a wide variety of risks that threaten the security of corporate information assets. Information risks need to be brought under control and IT Risk Management plays a role in mitigating the technology-related risks to information. However, information is not only exposed to IT-related risks, therefore, proper Information Security efforts are required beyond those that merely mitigate IT-related risks. Organizations must strive to implement Information Security effectively and ensure it supports their business goals and the interests of the shareholders.

There needs to be strong board-level support for the Information Security function through sound Information Security Governance efforts to align it with the goals and objectives of the organization. These efforts will ensure organizations uphold shareholder interests, organizational goals and objectives and demonstrate due care and due diligence which is necessary to satisfy organizational compliance with legal and regulatory requirements. The BoD needs clear direction to implement Information Security Governance effectively. This dissertation proposed a framework for Information Security Governance to facilitate the BoD in exercising sound Information Security Governance, thereby, demonstrating due care and due diligence for Information Security.

The BoD needs to be aware of the many risks that IT presents, including IT-related information risks because IT plays a major role in enabling an organization to achieve its business objectives. It was stated previously that IT seems to be a neglected topic at board level. This can weaken organizational Information Security Governance efforts because IT has a significant role to play in the storage, transmission and processing of information assets. Sound IT Governance efforts are required at board level to ensure that IT and IT strategy support the organizational business goals and objectives,

which include goals and objectives for Information Security. This dissertation motivated the importance of the IT Oversight Committee since the BoD appears to lack adequate knowledge and expertise to facilitate accurate IT decision making. The IT Oversight Committee has the knowledge and expertise to advise to BoD on appropriate IT strategy and ensures that such strategy supports Information Security.

The arguments presented above form the basis of this study. The following section presents a summarized account of each chapter and helps to motivate the main argument of the study.

8.2 Summary

Chapter 1 introduced the concept of Information Security and highlighted the various problems that needed to be considered. It was noted that Information Security is viewed from a technical point of view. However, some authors claim that Information Security is a legal and strategic concern and a Corporate Governance issue. These arguments form the basis around which the study was conducted. These arguments support the main objective of the study which was to develop an Information Security Governance framework that provides information-risk-related information into the Corporate Governance framework. An additional objective was to demonstrate the importance of the IT Oversight Committee to advise the BoD on matters of IT and IT-related risks to information. The methodology of the study was an in-depth literature survey focusing on the field of Information Technology and Information Security. The methodology included the development of the framework for Information Security Governance and the argument supporting the necessity of the IT Oversight Committee.

General Risk Management and Corporate Governance were the topic of ***Chapter 2***. An overview of the concept of risk was presented to define the concept, its various key areas and how it should be dealt with. It was noted that risk is currently perceived with a negative connotation and it is commonly dealt with through the process of Risk Management. Risk Management, in general, was discussed to define it and where it originated from. Various strategies for implementing Risk Management were discussed together with various Risk Management supportive activities, like Risk Anal-

ysis, which plays an important role in identifying, estimating and evaluating risk. Risk Management forms an important part of the Corporate Governance function of an organization which was discussed in detail. It ensures that Corporate Governance is able to achieve its main objective of preserving shareholder interests. This is accomplished by enabling the BoD to direct and control the organization effectively to avoid, accept, transfer and mitigate risks within their risk appetite. The relationship between Risk Management and Corporate Governance was explained together with the importance of Risk Management as a Corporate Governance responsibility. This chapter concluded that Risk Management has a significant IT component due to the vast organization-wide implementation of IT.

Information technology risk should be managed through proper IT Risk Management practices. The concept of Risk Management from an IT perspective was discussed in ***Chapter 3***. The chapter began with a discussion about the use of IT in an organization in terms of the growth in dependence on IT, why IT is important for business success and what risks are associated with the utilization of IT. The process of IT Risk Management was discussed to demonstrate how the IT-related risks of the organization are dealt with effectively. Various strategies for IT Risk Management were discussed and some examples of these, i.e. the CCTA's Risk Analysis and Management Methodology (CRAMM) and Livermore Risk Analysis Methodology (LRAM), were elaborated upon. The importance of IT Risk Management was motived and the chapter concluded that IT Risk Management plays an important role in Information Security.

Information Security is essential to ensure that all aspects of risk, including technology-related risk, to information are addressed successfully. ***Chapter 4*** elaborated on the management of Business Information Security and commenced with a discussion about business information in general. It was noted that business information includes any type of information, not only in electronic form, and is exposed to technology, people and business processes that threaten its characteristics. These characteristics include its confidentiality, integrity and availability. Business information risk was discussed in detail and it was noted that risks occur internally and externally to an organization from human, technical and natural sources. Information Security aims to mitigate the information risks that arise from these sources.

Information Security was discussed in detail to define it and explain the necessity of dealing with information-related risks. Information Security is implemented through the process of Information Security Management (ISM), which was discussed and it was explained how ISM can be implemented based on the guidance of accepted standards and security codes of practice such as ISO/IEC 17799. The chapter concluded that ISM emphasizes the criticality of business information which requires board-level attention.

The criticality of business information requiring board-level attention, demonstrates the need for Information Security Governance. ***Chapter 5*** discussed Information Security Governance in detail. The chapter explored the current state of Information Security in most organizations. It was noted that Information Security appears to lack necessary board-level attention because it is often viewed as a technology issue to be handled at the department level. It should, however, be a fundamental responsibility of the BoD and the chapter discussed the various considerations the BoD needs take into account to ensure that Information Security remains effective. The BoD should exercise due care and due diligence for Information Security and comply with the legal and regulatory requirements that are applicable to their organization. The Corporate Information Security Policy is essential to ensure that the objectives of the BoD for Information Security are communicated to the entire organization. Information Security requires a policy-driven approach ensuring that it remains effective and this begins at board level through sound Information Security Governance efforts. Information Security Governance was discussed in detail to highlight its components, motivate its importance and differentiate it from the Information Security Management function. The framework for Information Security Governance was proposed to help guide the BoD in their Information Security Governance endeavors once Information Security Governance had been motivated. The framework was motivated by arguing its necessity and demonstrating its implementation. Additionally, various Information Security tasks, roles and responsibilities were covered. These ensure that key role players in the broader Information Security function understand what they are accountable and responsible for. The benefits of Information Security Governance were highlighted to strengthen the argument regarding the necessity of an Information Security Governance framework. The chapter concluded that

Information Security Governance requires IT to be addressed effectively at board level.

Information technology issues are best addressed at board level through effective IT Governance. IT Governance was the topic of discussion in ***Chapter 6*** of the dissertation. The chapter covered need for good Corporate Governance and highlighted some prominent Corporate Governance failures, specifically that of Enron Corp. and Worldcom Inc. resulting from improper accounting practices. It was noted that should organization's not consider IT with nearly the same importance as matters of finance, situations similar to those that transpired at Enron Corp. and Worldcom Inc. may re-occur. The criticality of IT was stressed together with several factors that inhibit the effective use of IT in an organization to motivate this more clearly. One of these inhibiting factors include a lack of a close relationship between the business and its IT resources. This is because many organizations do not have proper governance structures in place to facilitate IT-business alignment. The BoD has a fundamental responsibility to ensure that IT is appropriately and effectively applied to reduce risk and reap acceptable returns on IT investment. This can be achieved by applying a formalized governance framework that enables the BoD to give effective IT direction and control. IT Governance was discussed and it was demonstrated how it enables the BoD to govern the use of IT effectively by implementing the specifications of an IT control framework such as COBIT. Some benefits of IT Governance were discussed and the chapter concluded that good IT Governance requires that the BoD make well-informed decisions with relation to IT.

Good IT decision making requires board-level IT oversight. The concept of IT oversight was discussed at length in ***Chapter 7*** and the necessity of the board-level IT Oversight Committee was argued. The chapter discussed the IT Governance failures of some prominent organizations such as Nike, Disney, Kmart and Gateway. The responsibility for board-level IT guidance was explored, after scrutinizing these IT Governance failures, specifically regarding whose this responsibility is. Board committees were explored particularly highlighting their importance in answering this question. The duties of the Audit Committee, the Remuneration Committee and the Risk Management Committee were discussed. It was established that these committees do not necessarily have the required skills to provide adequate board-level advice.

Therefore, the need for the IT Oversight Committee was argued and its proposed function and composition were discussed. The difference between an IT Oversight Committee and IT Steering Committee was addressed to support the argument for the need for an IT Oversight Committee at board level. The chapter concluded by stating that IT oversight is important in enabling Information Security Governance and IT Governance to remain effective and preserve critical business information assets.

The various chapters of this study helped support the main argument. It is, however, important to understand how this was accomplished and how the resolution to the primary research problem was attained.

8.3 Solving the Problem

The primary research problem for this dissertation was stated as: "What steps are needed to create an effective Information Security Governance framework that can be integrated into the overall Corporate Governance program and ensure that the BoD is able to make well-informed decisions relating to IT to address all aspects of business information risk effectively?". This problem statement helped define the primary objective of the study which was to develop such an Information Governance Framework as well as demonstrate the importance of the IT Oversight Committee to advise the BoD on matters of IT and IT-related information risks.

A number a secondary objectives were defined to help accomplish the primary objective of the study and provide a resolution to the problem statement.

The first of these secondary objectives was: The positioning of information-related risks within the broader Risk Management framework. The dissertation achieves this objective by demonstrating that Enterprise Risk Management, which is a Corporate Governance responsibility, must ensure that all risks that threaten the continued operations of the organization are managed to an adequate level to protect shareholder interests. Information plays a major role in enabling an organization to attain a competitive advantage and its use is facilitated by the implementation of Information technology. The strategic application of technology to exploit information appropriately can produce business value and shareholder returns, but, equally presents numer-

ous risks. Therefore, information risk, which includes IT-related information risks, should be addressed through various Information Risk Management efforts to ensure that Enterprise Risk Management is complete and effective.

The second of these secondary objectives was: The relation of information risks to IT risks. This objective was accomplished by demonstrating that information risk is far wider than IT, therefore, merely considering IT Risk Management to address information risks is not sufficient to ensure the full protection of information. There must be consideration for natural and human risks to information as well as the technology risks. These risks are addressed by considering various Information Security requirements. These include requirements to protect the IT infrastructure, legal, regulatory and statutory requirements and business requirements for confidentiality, integrity and availability. These together with the guidance of industry codes of practice, such as ISO/IEC 17799, help address all aspects of information risk effectively.

The final secondary objective was: The recognition of a means to identify risk related information which will assist in the governance of IT risks. This objective was accomplished by discussing the importance of IT as a strategic resource. It is the responsibility of the BoD to ensure that all critical systems support the strategic business objectives of the organization, including Information Security. The BoD needs to ensure that an effective IT Governance function is in place to achieve the alignment of IT with the business and reduce the risks that IT presents. However, it was noted that the BoD appears to lack the necessary skills to direct and control the use of IT effectively. Therefore, the IT Oversight Committee at board-level was proposed to advise the BoD on technology issues and provide them with the information necessary to enable them to apply IT strategically in a manner that produces business value and reduces IT-related risks, including those to information.

These three secondary objectives enabled the primary objective to be accomplished by demonstrating that information Risk Management forms part of the wider functions of Information Security Management. Information Security Management enables the mitigation of information-related risks, however, the Information Security strategy that enables Information Security Management to be a success needs to be defined at board-level through

effective Information Security Governance efforts. The BoD appears to lack the necessary insights to direct and control Information Security effectively. Therefore, they require a governance framework to help guide them in their Information Security endeavors. This framework demonstrates, to the BoD, the scope of protecting information assets and highlights the key security requirements identified through achieving the secondary objectives. These security requirements together with the help of the IT Oversight Committee ensure that the Information Security Governance framework provides information-risk-related information into the Corporate Governance framework to address all aspects of business information risk effectively.

The primary objective of this dissertation is to prove that research methods can be used effectively to solve a research problem. The argued solution in this case was an integration and contextualization of related literature to solve the stated problem and meet the objectives set.

8.4 Conclusion

Information is an important asset in most organizations and it produces significant business value if it is kept confidential, accurate and complete and is available when needed. There needs to be an organization-wide commitment to Information Security starting with the BoD to ensure that these characteristics of information are preserved. The BoD must be aware of what they need to consider to ensure that information remains secure. The framework for Information Security Governance and the IT Oversight Committee can play a fundamental role in facilitating the BoD in their governance efforts over Information Security. However, further research would involve spending more time clearly mapping out the organizational structures for Information Security tasks, roles and responsibilities and the composition of and skills required by the personnel who form the IT Oversight Committee. Nonetheless, Information Security is a journey and not a destination and requires continuous improvement over time with clear direction and control through sound governance efforts.

References

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

BambooWeb Dictionary Open Content Encyclopedia. (2005a). *Board of Directors.* Available from: `http://www.bambooweb.com/articles/b/o/Board_of_directors.html`.

BambooWeb Dictionary Open Content Encyclopedia. (2005b). *Chairman.* Available from: `http://www.bambooweb.com/articles/c/h/Chairman.html`.

BambooWeb Dictionary Open Content Encyclopedia. (2005c). *Chief Executive Officer.* Available from: `http://www.bambooweb.com/articles/c/e/CEO.html`.

BambooWeb Dictionary Open Content Encyclopedia. (2005d). *Fiduciary Duty.* Available from: `http://www.bambooweb.com/articles/f/i/Fiduciary_duty.html`.

BambooWeb Dictionary Open Content Encyclopedia. (2005e). *Shareholder.* Available from: `http://www.bambooweb.com/articles/s/h/Shareholder.html`.

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

Baskerville, R. (1993). Information systems security design methods: implications for information systems development. *ACM Computing Surveys (CSUR)*, *25*(4), 375–414.

BDO. (1999). Available from: http://www.bdo.co.za/infoCentre/publications/corporate_governance/governance.htm.

Bergamo, P. (2005). *Setting the direction.* Available from: http://www.deltacorp.com/lib/getfile.asp?ID=54.

Birman, K. P. (2000). The next-generation internet: Unsafe at any speed. *IEEE Computer*, *33*(8), 54–60.

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

Borland Software Corporation. (2005, March). *Understanding and Managing Risk.* Available from: http://wp.bitpipe.com/resource/org_982697212_431/Understanding_Managing_Risk-Borland_In_Network.pdf.

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

Burnie, D. (2003). *Science.* Available from: http://encarta.msn.com/text_761557105_1/Science.html: Microsoft Encarta Online Encyclopedia 1997/2003.

Busch-Vishniac, I. (2001). *Introducing the Johns Hopkins University Information Security Institute: the need, the vision, the future.* Available from: http://www.jhuisi.jhu.edu/institute/docs/JHUISI_1-21-01.pdf.

Business Software Alliance. (2004). *Information Security Governance: Toward a Framework for Action.* Available from: http://www.bsa.org/resources/loader.cfm?url=/commonspot/security/getfile.cfm&pageid=5841&hitboxdone=yes.

Cadbury Report. (1992). *Report of the Committee on the Financial Aspects of Corporate Governance.* Available from: http://www.ecgi.org/codes/documents/cadbury.pdf.

Carlton Collins, J. (2003). *Supply Chain Insights.* Available from: http://www.accountingsoftwareadvisor.com/ec/supplychain.htm.

Changepoint Corporation. (2004). *Governance: The Board's - and the CIO's - Business.* Available from: `http://itresearch.forbes.com/detail/RES/1081531053_905.html`.

Cho, S., & Ciechanowicz, Z. (2001). Checklist-based risk analysis with evidential reasoning. In M. Dupuy & P. Paradinas (Eds.), *IFIP TC11 16th international conference on information security (IFIP/Sec'01).* Kluwer Academic Publishers.

Citadel Security Software, Inc. (2005). *Evolving IT Risk Management From Tactical To Strategic.* Available from: `http://www.sans.org/rr/whitepaper/threats/12.php`.

COBIT. (2000). *COBIT Framework* (Third ed.). Available from: `https://www.isaca.org/TemplateRedirect.cfm?template=/MembersOnly.cfm&ContentID=13059`: COBIT Steering Committee and the IT Governance Institute.

Corporate Governance Task Force. (2004, April). *Information Security Governance: A Call To Action.* Available from: `http://www.cyberpartnership.org/InfoSecGov4_04.pdf`.

COSO. (2004). *Enterprise Risk Management - Integrated Framework, Vol. 1 and Vol. 2.* Available from: `http://www.coso.org`.

Cule, P., Schmidt, R., Lyytinen, R., & Keil, M. (2000). Strategies for Leading off IS Project Failure. *Information Systems Management*, *Spring*, 65 – 73.

Deloitte and Touche. (2002). *Management briefing - information security.* Available from: `http://www.deloitte.com/dtt/cda/doc/content/info_security(1).pdf`.

Douglas, M. (1990). Risk as a forensic resource. *Daedalus*, *119*(4), 1–17.

Douglas, M. (1992). Risk and blame. In *Risk and blame: Essays in cultural theory* (pp. 3–21). Routledge.

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

Entrust. (2004a). *Information Security Governance (ISG): An Essential Element of Corporate Governance.* Available from: http://itresearch.forbes.com/detail/RES/1082396487_702.html.

Entrust. (2004b). *Protecting Your Most Important Asset: Information: How Data Security Mitigates Risk and Enables Compliance.* Available from: https://www.entrust.com/contact/index.cfm?action=wpdownload&tpl=resources&resource=secure_data_wp.pdf&id=21157&bp=ou812.

Entrust, Inc. (2004, July). *Implementing Information Security Governance (ISG).* Available from: http://itresearch.forbes.com/detail/RES/1090863380_986.html.

Exler, R. (2003). *IT Goveranance Frameworks.* Available from: http://www2.cio.com/analyst/report1559.html.

Flynn, I. M., & McIver McHoes, A. (1997). Understanding operating systems. In (Second ed., pp. 3 – 16). PWS Publishing.

Frosdick, S. (1997). The techniques of risk analysis are insufficient in themsleves. *Disaster Prevention and Management: An International Journal*, *6*(3), 165–177.

Furnas, D. R. (2004). *Due care or do not care?* Available from: http://www.issa-sac.org/info_resources/Due_Care_5-13-04.shtml.

Gamma Secure Systems Limited (Ed.). (1997). *A practitioner's view of cramm.* Available from: http://www.gammassl.co.uk/topics/hot.html: Gamma Secure Systems Limited.

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

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

Girard, K. (2002). *Three big breakdowns of 2001.* Available from: http://www.findarticles.com/p/articles/mi_zdbln/is_200201/ai_ziff21763.

Gordon, & Glickson. (2001). *Comprehensive information security policies: meeting an organization's privacy and security needs.* Available from: `http://www.ggtech.com/`.

Gordon, G. (2002). *Dozens of threats beset your data. sunday times, business surveys.* Available from: `http://www.suntimes.co.za/2002/05/12/business/surveys/internet/survey10.asp`.

Grant, G. H. (2003). The evolution of corporate governance and its impact on modern corporate america. *Management Decision*, *41*(6), 923–934.

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

Health and Safety Executive. (1988). *The Tolerability of Risk from Nuclear Power Stations.* HMSO.

Hoffman, T. (2004). *IT Oversight Gets Attention at Board Level.* Available from: `http://www.computerworld.com/industrytopics/transportation/story/0,10801,93178,00.html`.

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

Institute of Directors of Southern Africa. (2002). *Corporate Governance.* Available from: `http://www.iodsa.co.za`.

ISO/IEC 17799. (2005). *Information technology - security techniques - code of practice for information security management* (Tech. Rep.). ISO/IEC.

ISO/IEC TR 13335-1. (2004). *Information Technology - Security techniques - Management of information and communications technology security Part 1: Concepts and models for information and communications technology security management* (Tech. Rep.). ISO/IEC.

ISO/IEC TR 13335-3. (1998). *Information technology - Guidelines for the management of IT security Part 3: Techniques for the management of IT security* (Tech. Rep.). ISO/IEC.

IT Governance Institute. (2003). *Board Briefing on IT Governance.* Available from: http://www.isaca.org/Content/ContentGroups/ITGI3/Resources1/Board_Briefing_on_IT_Governance/26904_Board_Briefing_final.pdf.

IT Governance Institute. (2004). *IT Strategy Committee.* Available from: http://www.ITgovernance.org/resources.htm.

IT Governance Institute. (2005a). *The ceo's guide to it value @ risk.* Available from: http://www.itgi.org/template_ITGI.cfm?template=/ContentManagement/ContentDisplay.cfm&ContentID=20697.

IT Governance Institute. (2005b). *It governance executive summary.* Available from: http://www.itgi.org/template_ITGI.cfm?template=/ContentManagement/ContentDisplay.cfm&ContentID=19976.

IT Governance Institute. (2005c). *IT Governance Domain Practices and Competencies - IT Alignment: Who Is in Charge?* Available from: http://www.itgi.org/template_ITGI.cfm?template=/ContentManagement/ContentDisplay.cfm&ContentID=22247.

IT Governance Institute. (2005d). *IT Governance Domain Practices and Competencies - Information Risks: Whose Business Are They?* Available from: http://www.itgi.org/template_ITGI.cfm?template=/ContentManagement/ContentDisplay.cfm&ContentID=21447.

IT Governance Institute. (2005e). *Information Security Governance: Guidance for Boards of Directors and Executive Management.* Available from: http://www.isaca.org/ContentManagement/ContentDisplay.cfm?ContentID=15998.

Jennings, T. (2004, March). *Change Management: An Essential Tool for IT Governance.* Available from: http://www.merant.com/Shared/pdfs/dimensions/CM_for_IT_Governance.pdf.

Jung, C., Han, I., & Suh, B. (1999). Risk analysis for electronic commerce using case-based reasoning. *International Journal of Intelligent Systems in Accounting, Finance and Management*, *8*.

Keen, P. G. W. (1991). *Shaping the future: Business design through information technology.* Cambridge: Harvard Business School Press.

King Report. (2001). *The King Report on Corporate Governance for South Africa.* Available from: `http://www.iodsa.co.za/IoD%20Draft%20King%20Report.pdf`.

Kirkwood, A. S. (1994). Why do we worry when scientists say there is no risk? *Disaster Prevention and Management: An International Journal*, *3*(2).

Kontio, J., Getto, G., & Landes, D. (1998). Experiences in improving risk management processes using the concepts of the riskit method. In *Proceedings of the 6th acm sigsoft international symposium on foundations of software engineering* (pp. 163 – 174). ACM Press.

Kwok, L. for, & Longley, D. (1999). Information security management and modelling. *Information Management and Computer Security*, *7*(1), 30–40.

Lichtenstein, S. (1996). Factors in the selection of a risk assessment method. *Information Management and Computer Security*, *4*(4), 20 – 25.

Luftman, J. N., Papp, R., & Brier, T. (1999). Enablers and inhibitors of business-IT alignment. *Communications of the Association for Information Systems*, *1*(11).

Mayo, D., & Hollander, R. (1991). Introduction to Part II - Uncertain Evidence in Risk Management. In D. Mayo & R. Hollander (Eds.), *Acceptable evidence: Science and values in risk management* (pp. 93–8). Oxford University Press.

McKoen, P., & Gough, L. (1997). *The financial manual for non-financial managers.* Pitman Publishing.

Mellon Financial Corporation. (2004). *Charter of the Technology Committee of the Board of Directors.* Available from: `http://www.mellon.com/governance/pdf/technology.pdf`.

Moses, R. H. (1992). Risk analysis and management. In K. M. Jackson & J. Hruska (Eds.), *Computer security reference book.* Butterworth-Heinemann.

Msomi, S. (1999). *Survey shows apathy over information safety policies. sunday times, business times.* Available from: http://www.btimes.co.za/99/1114/comp/comp08.htm.

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

New York Stock Exchange. (2001). *The investing public.* Available from: http://www.nyse.com/pdfs/2001_factbook_05.pdf.

Nolan, R. (2004). *Richard Nolan: A Committee of One's Own.* Available from: http://www.cioinsight.com/article2/0,1397,1529279,00.asp. (News Story By Allen E. Alter)

OASIS. (2002). Available from: http://ssdoo.gsfc.nasa.gov/nost/isoas/presentations/USDA_19990219/tsld013.htm.

O'Brien, J. A. (2000). Introduction to information systems: Essentials for the internetworked enterprise. In (pp. 3 – 46). Irwin/McGraw-Hill.

Peterson, R. (2003). Information strategies and tactics for information technology governance. In *Strategies for information technology governance.* Idea Group Publishing.

Preventsys. (2005, February). *Managing Enterprise IT Security Risk: Get Ahead Of the Problem.* Available from: http://knowledgestorm.co.nz/shared/write/collateral/WTP/50089_28266_14730_!QVM6MA007HICPreventsys_-_Enterprise_Risk_Management_for_Infosecurity.pdf?ksi=930509&ksc=1217805593.

Priest, G. (1990). The new legal structure of risk control. *Daedalus*, *119*(4), 207–28.

Risk Management Research Laboratory Overview. (2003). Available from: http://undergroundnews.com/files/texts/underground/hacking/risktool.htm.

Ritchie, B., & Brindley, C. (2001). The information-risk conundrum. *Marketing Intelligence and Planning*, *19*(1), 29–37.

Royal Society. (1992). *Risk: Analysis, Perception and Management* (Report of a Royal Society Study Group). The Royal Society.

Schneider, G. P., & Perry, J. T. (2001). Electronic commerce. In (Second ed., pp. 193 – 236). Course Technology.

Schoenberg, C. (2005). *Why due diligence as a defense is not enough.* Available from: `http://www.net-security.org/article.php?id=777`.

Scottsdale Institute. (2001). *Closing the governance gap: Bringing boards into the it equation.* Available from: `http://www.itgi.org/template_ITGI.cfm?template=/ContentManagement/ContentDisplay.cfm&ContentID=6651`.

SecureSynergy SecurityScape. (2003, June). *Policing Systems Assets Through Infosec Policies.* Available from: `http://www.securesynergy.com/library/articles/073-2003.php`.

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

Slovic, P. (1991). Beyond numbers: a broader perspective on risk perception and risk communication. In D. Mayo & R. Hollander (Eds.), *Acceptable evidence: Science and values in risk management* (pp. 99–114). Oxford University Press.

Smith, M. R. (1989). *Commonsense computer security.* McGraw-Hill.

Strutt, J. (1993). *Risk assessment and management: The engineering approach.* (Center for Industrial Safety and Reliability, Cranfield University)

Swindle, O., & Conner, B. (2004, May). *The Link Between Information Security and Corporate Governance.* Available from: `http://www.computerworld.com/securitytopics/security/story/0,10801,92915,00.html`.

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

Thomson, K., & von Solms, R. (2003). *Integrating information security into corporate culture.* Masters dissertation, Nelson Mandela Metropolitan University, Port Elizabeth, South Africa.

TIAA-CREF. (1998). *Policy Statement for Corporate Governance.* Available from: `http://www.tiaa-cref.org/pressroom/corpgov.pdf`.

Trillium Software. (2004). *Corporate Governance and Compliance: Could Data Quality Be Your Downfall?* Available from: `http://www.trilliumsoftware.com/success/dqic.pdf`.

Turn, R. (1986). Security and privacy requirements in computing. In *Proceedings of 1986 fall joint computer conference on fall joint computer computer conference* (pp. 1106–1114). IEEE Computer Society Press.

URN 99/704 (NEW). (1999). *Information your most valuable asset. Protect it.* Department of trade and industry.

Valsamakis, A. C., Vivian, R. W., & du Toit, G. S. (1992). *The theories and principles of risk management.* Butterworths.

Van Grembergen, W. (2002). Introduction to the minitrack it governance and its mechanisms. In *Proceedings of the 35th hawaii international conference on system sciences (hicss).*

Vericept Corporation. (2004). *Preventing Identity Theft and Loss of Intellectual Property: The Importance of Information Security in Internal Controls and Corporate governance.* Available from: `http://www.vericept.com/Downloads/WhitePapers/Vericept_Fraud_IdentityTheft_WP.pdf`.

Vinten, G. (2002). The corporate governance lessons of enron. *Corporate Governance: International Journal of Business in Society*, *2*(4), 4–9.

von Solms, B. (2001). Corporate governance and information security. *Computers and Security*, *20*(3), 215–218.

Warner, F. (1993). Calculated Risks. In *Science and public affairs* (pp. 44–9).

Webb, S., & Robertson, M. (2004). *Enabling IT Governance with Project Portfolio Management.* Available from: `http://itresearch.forbes.com/data/document.do?res_id=1088617963_260`.

Weill, P., & Woodham, R. (2002). *Don't just lead, govern: Implementing effective it governance.* Available from: `http://ideas.repec.org/p/mit/sloanp/4237-02.html`.

Whitman, M. E., & Mattord, H. J. (2003a). Principles of information security. In (pp. 153 – 190). Course Technology.

Whitman, M. E., & Mattord, H. J. (2003b). Principles of information security. In (pp. 117 – 152). Course Technology.

Whitman, M. E., & Mattord, H. J. (2003c). Principles of information security. In (pp. 191 – 234). Course Technology.

Whitson, G. (2003). Computer security: theory, process and management. *J. Comput. Small Coll.*, *18*(6), 57 – 66.

Williams, C. A., Smith, M. I., & Young, P. C. (1998). *Risk management and insurance.* Irwin McGraw Hill.

Williams, P. (2001). Information security governance. *Information Security Technical Report*, *6*(3), 60–70.

Wills, M. (1999). personal communication. In *Urn 99/699 (new). protecting business information - overview.* Department of Trade and industry.

Wold, G. H., & Shriver, R. F. (Eds.). (1997). *Risk analysis techniques.* Available from: `http://www.drj.com/new2dr/w3_030.htm`: Systems Support, inc.

World Bank Group. (1999, September). *Corporate Governance: A Framework for Implementation.* Available from: `http://www.worldbank.org/html/fpd/privatesector/cg/docs/gcgfbooklet.pdf`.

Yazar, Z. (2002). *A qualitative risk analysis and management tool - CRAMM.* Available from: `http://www.sans.org/rr/whitepapers/auditing/83.php`.

Part V

Appendices

Appendix A

Papers Presented and Published

A.1 Paper 1

In June 2004, at the ISSA Conference held in Johannesburg, South Africa, Shaun presented the paper titled "Risk Management Vs The Management of Risk: Does It Matter to the Board?".

Abstract

This paper addresses the effectiveness of risk management from an information protection perspective when reporting on risks to an organization's board of directors is concerned. Firstly, the concept of risk management in general is defined in order to clarify its intended purpose. Then the capabilities of risk management from an IT perspective are highlighted as far as the protection of information is concerned. The paper further points out that according to the King Report on Corporate Governance risk management is the responsibility of the board, but risk management from an information protection perspective is unable to address the full scope of the requirements of the board in this regard. It is further noted that there is a difference between what is termed risk management and the management of risk. Hence, it is argued that the board's responsibilities are in fact concerned with the management of risk and not risk management.

Reference

Posthumus, S., & von Solms, R. (2004). Risk Management Vs The Management of Risk: Does It Matter to the Board?. In *Proceedings of the ISSA enabling tomorrow Conference 2004* (on CD).

A.2 Paper 2

In December 2004, the paper titled "A Framework for the Governance of Information Security" was published in the *Computers & Security* journal.

This paper, according to a survey conducted by ScienceDirect Digital Library, was 2nd in the "TOP25 Hottest Articles" in the *Computers & Security* journal for the 3rd quarter of 2005 based on downloads and views.

Abstract

This paper highlights the importance of protecting an organization's vital business information assets by investigating several fundamental considerations that should be taken into account in this regard. Based on this, it is illustrated that information security should be a priority of executive management, including the Board and CEO and should therefore commence as a corporate governance responsibility. This paper, therefore, motivates that there is a need to integrate information security into corporate governance through the development of an information security governance (ISG) framework. This paper further proposes such a framework to aid an organization in its ISG efforts.

Reference

Posthumus, S., & von Solms, R. (2004). A framework for the governance of information security. *Computers & Security, 23*(8), 638-646.

A.3 Paper 3

In April 2005, the paper titled "IT Oversight: An Important Function of Corporate Governance" was published in the *Computer Fraud & Security* journal.

Abstract

This paper discusses the need for greater board level participation in the way an organization is directed and controlled, with specific interest in IT related issues. IT has become widely integrated into most organizations but IT issues remain a neglected topic at board level. The general failure by the board to effectively strategically direct and control IT is derived from a lack of adequate skills and insight into IT related issues at board level. Therefore this paper motivates the institution of an IT oversight committee to help advise the board in terms of IT governance and other strategic IT-related issues, and thereby bring about a stronger system internal control and an enhanced approach to corporate governance.

Reference

Posthumus, S., & von Solms, R. (2005). IT Oversight: An Important Function of Corporate governance. *Computer Fraud & Security, 6*, 11-17.

A.4 Paper 4

In December 2005, at the IFIP TC-11 WG 11.1 & WG 11.5 Joint Working Conference on Security Management, Integrity, and Internal Control in Information Systems, Fairfax, Virginia, USA, Shaun presented the paper titled "A Responsibility Framework for Information Security"

Abstract

This paper demonstrates that information security is more than a technical issue, through the development of an information security responsibility framework that shows consideration for strategic and legal issues as well. It is important that information security be viewed as both a governance challenge and a management responsibility. In order to achieve this this paper addresses information security governance and the board's participation in directing and controlling security efforts. Furthermore information security management is addressed in order to demonstrate how information security should be implemented. Once a comprehensive picture of the information security function has been established, the roles of various individuals in

terms of information security are discussed and mapped out in the responsibility framework in order to demonstrate the true scope of an organizations information security function.

Reference

Posthumus, S., & von Solms, R. (2004). A Responsibility Framework for Information Security. In *Proceedings of the IFIP TC-11 WG 11.1 & WG 11.5 Joint Working Conference on Security Management, Integrity, and Internal Control in Information Systems* (pp. 205-221). Springer.