Integrating Information Security into Corporate Culture

Kerry-Lynn Thomson
Integrating Information Security into Corporate Culture

This dissertation comprises research work completed in the field of

INFORMATION TECHNOLOGY

and is submitted by

KERRY-LYNN THOMSON

in accordance with the requirements for the degree of

MAGISTER TECHNOLOGIAE : INFORMATION TECHNOLOGY

at the

PORT ELIZABETH TECHNIKON

Promoter: PROFESSOR R. VON SOLMS
Year: 2003
My sincerest gratitude to the following people:

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

My family
for their encouragement and belief in me.

And above all,
to my Creator who made it possible.
# Table of Contents

**Chapter 1: Introduction** ................................................................. 1  
1.1 Introduction ................................................................................. 1  
1.2 Problem Statement ................................................................. 2  
1.3 Objectives ................................................................................. 3  
  1.3.1 Primary Objective ............................................................... 3  
  1.3.2 Secondary Objective ......................................................... 3  
1.4 Methodology ............................................................................. 4  

**Chapter 2: Information Security** .................................................. 6  
2.1 Introduction ............................................................................. 6  
2.2 Background ............................................................................. 7  
2.3 What is Information Security? ................................................ 9  
  2.3.1 The Importance of Information Security ......................... 10  
  2.3.2 Effects of Inadequate Information Security ................... 11  
2.4 Essential Pillars of Information Security ............................... 13  
2.5 Problems with Information Security ....................................... 15  
2.6 Conclusion ............................................................................. 15  

**Chapter 3: Corporate Governance** .............................................. 17  
3.1 Introduction ........................................................................... 17  
3.2 King Report on Corporate Governance ................................. 18  
3.3 Corporate Governance ........................................................ 19  
  3.3.1 Importance of Corporate Governance ......................... 20  
  3.3.2 Corporate ‘Sins’ ............................................................... 22  
  3.3.3 Essential Pillars of Corporate Governance ................... 23  
  3.3.4 Supporting Pillars of Corporate Governance ................ 25  
3.4 The Structure of Corporate Governance ............................... 26  
  3.4.1 Board of Directors .......................................................... 27
<table>
<thead>
<tr>
<th>Chapter 8: Information Security Obedience</th>
<th>89</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1 Introduction</td>
<td>89</td>
</tr>
<tr>
<td>8.2 Relationship between Information Security and Corporate Governance</td>
<td>90</td>
</tr>
<tr>
<td>8.3 Relationship between Corporate Governance and Corporate Culture</td>
<td>93</td>
</tr>
<tr>
<td>8.4 Relationship between Information Security and Corporate Culture</td>
<td>97</td>
</tr>
<tr>
<td>8.5 Relationships between the Three Fields</td>
<td>100</td>
</tr>
<tr>
<td>8.6 Information Security Obedience</td>
<td>106</td>
</tr>
<tr>
<td>8.7 Conclusion</td>
<td>108</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 9: Conclusion</th>
<th>110</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.1 Introduction</td>
<td>110</td>
</tr>
<tr>
<td>9.2 Summary</td>
<td>111</td>
</tr>
<tr>
<td>9.3 Solving the Problem</td>
<td>113</td>
</tr>
<tr>
<td>9.4 Further Research</td>
<td>114</td>
</tr>
<tr>
<td>9.5 Conclusion</td>
<td>115</td>
</tr>
</tbody>
</table>

| References                             | 118 |

| Appendix A1: Papers Presented and Published | 124 |
| Appendix A2: Article                    | 125 |
List of Figures and Tables

Figures

Chapter 1: Introduction
1.1 Rough draft of the proposed model .................................................. 4
1.2 Outline of chapters in dissertation ...................................................... 5

Chapter 8: Information Security Obedience
8.1 Information security protection depends on user behaviour and actions .......... 90
8.2 Responsibility of senior management for information security ...................... 91
8.3 The relationship of the Corporate Information Security Policy ..................... 92
8.4 The relationship between corporate governance and information security ....... 93
8.5 Corporate culture determines employee behaviour .................................... 94
8.6 Senior management outlines the vision for an organisation ........................ 95
8.7 The relationship of general management policies ..................................... 95
8.8 The relationship between corporate governance and corporate culture .......... 96
8.9 The relationship between information security and corporate culture influenced by a Corporate Information Security Policy .............................................. 99
8.10 The relationship between information security and corporate culture ........... 100
8.11 The relationships between information security, corporate governance and corporate culture ................................................................. 103
Tables

Chapter 8: Information Security Obedience

8.1 Effects of unacceptable information security, corporate governance and corporate culture ................................................................. 101
8.2 Effects of acceptable information security, corporate governance and corporate culture ................................................................. 102
Chapter 1: Introduction

1.1 Introduction

There are many components that are required for an organisation to be successful in its chosen field. These components vary from corporate culture, to corporate leadership, to effective protection of important assets. These and many more contribute to the success of an organisation.

One component that should be a definitive part in the strategy of any organisation is information security. Information security is one of the fastest growing sub-disciplines in the Information Technology industry, indicating the importance of this field (Zylt, 2001, online). Information security is concerned with the implementation and support of control measures to protect the confidentiality, integrity and availability of electronically stored information (BS 7799-1, 1999, p 1). Information security is achieved by applying control measures that will lessen the threat, reduce the vulnerability or diminish the impact of losing an information asset. However, as a result of the fact that an increasing number of employees have access to information, the protection of information is no longer only dependent on physical and technical controls, but also, to a large extent, on the actions of employees utilising information resources. All employees have a role to play in safeguarding information and they need guidance in fulfilling these roles (Barnard, 1998, p 12).

This guidance should originate from senior management, using good corporate governance practices. The effective leadership resulting from good corporate governance practices is another component in an organisation that contributes to its success (King Report, 2001, p 11). Corporate governance is defined as the exercise of power over and responsibility for corporate entities (Blackwell Publishers, 2000, online).

Senior management, as part of its corporate governance duties, should encourage employees to adhere to the behaviour specified by senior management to contribute
towards a successful organisation. Senior management should not dictate this behaviour, but encourage it as naturally as possible, resulting in the correct behaviour becoming part of the corporate culture.

If the inner workings of organisations are explored it would be found that there are many hidden forces at work that determine how senior management and the employees relate to one another and to customers. These hidden forces are collectively called the culture of the organisation (Hagberg Consulting Group, 2002, online). Cultural assumptions in organisations grow around how people in the organisation relate to each other, but that is only a small part of what corporate culture actually covers (Schein, 1999, p 28).

Corporate culture is the outcome of all the collective, taken-for-granted assumptions that a group has learned throughout history. Corporate culture is the residue of success. In other words, it is the set of procedures that senior management and employees of an organisation follow in order to be successful (Schein, 1999, p 29).

Cultivating an effective corporate culture, managing an organisation using efficient corporate governance practices and protecting the valuable information assets of an organisation through an effective information security program are, individually, all important components in the success of an organisation. One of the biggest questions with regard to these three fields is the relationship that should exist between information security, corporate governance and corporate culture. In other words, what can the senior management of an organisation, using effective corporate governance practices, do to ensure that information security practices become a subconscious response in the corporate culture?

1.2 Problem Statement

Effective information security today calls for widespread human interaction which involves everyone from senior management to all end-users. The necessary guidance and direction from senior management, in most cases, is not communicated properly to
employees and does not have a large influence on their understanding and involvement in effective information security.

Senior management does not usually influence employee behavior adequately to instill a corporate culture that is favourable for combating information security risks. In addition, employees, generally, are not provided with the required education, examples and role models that will shape a corporate culture into one that dictates their everyday secure handling of information.

1.3 Objectives
The purpose of this dissertation is to investigate the relationship between the three fields of information security, corporate governance and corporate culture.

1.3.1 Primary Objective
The primary objective of this dissertation is to investigate to what extent the senior management of an organisation should be involved in changing the beliefs, principles and practices of the employees towards information security, thereby influencing their behaviour positively towards the protection of information.

This investigation should lead to the development of a model depicting how the three fields of information security, corporate governance and corporate culture should be correlated. Based on this investigation, a term that encompasses the three fields of information security, corporate governance and corporate culture will be defined and motivated.

1.3.2 Secondary Objective
The secondary objectives are to investigate and clarify the relationships that should exist between, firstly, corporate governance and information security, secondly, corporate governance and corporate culture and lastly, information security and corporate culture.
1.4 Methodology

In response to these objectives, an extensive literature study will be conducted. The three fields of information security, corporate culture and corporate governance will be investigated individually and then in relation to one another, resulting in the integration of various related aspects within the three fields. Both the subtle and evident facets of corporate culture will be investigated and the importance of information security in the daily operation of an organisation will be explored. Corporate governance will be examined and the importance of this field to organisations will be highlighted. The responsibility that senior management has to both corporate culture and information security will be explored, together with the role that corporate governance plays in facilitating the link between corporate culture and information security.

Once the literature study has been completed and the data analysed, a model will be created, through solid arguments, to clearly explain the relationships between information security, corporate culture and corporate governance. A brief outline of the model is shown in Figure 1.1.

![Diagram](image_url)

*Figure 1.1. Rough draft of the proposed model*
‘A’ will represent the influence senior management has on the corporate culture of the organisation. ‘B’ will detail how the corporate culture affects the behaviour of senior management. ‘C’ will represent the need that exists for information security practices to receive guidance from senior management and ‘D’ will represent what senior management should do to take responsibility for information security. ‘E’ is the link that should exist for information security to become part of the corporate culture and ‘F’ will describe how corporate culture affects the behaviour of employees towards protecting information.

The first few chapters of the dissertation will investigate information security, corporate governance and corporate culture individually, and then investigate them in relation to one another. All three fields will then be related in further chapters. The following Figure 1.2 represents the layout of the chapters in this dissertation:
Chapter 2: Information Security

2.1 Introduction

Information is important. It is often described as the lifeblood of the emerging electronic economy (Gordon, 2002, online). No matter what the information entails; whether it is customer records, confidential documentation or financial information, there are many threats that make the information vulnerable (Gordon, 2002, online).

These threats to the security of the information come from many sources. Hackers and viruses often attack corporate computers and an organisation’s employee might inadvertently or maliciously cause a security breach (Gordon, 2002, online).

This chapter will investigate the evolution of Information Technology and information security, as well as investigate the importance of the role that information security plays.
in most organisations today. The important pillars of information security will be explored, as well as the current problems and misconceptions about information security. The consequences of inadequate levels of information security will also be investigated.

2.2 Background

The evolution of Information Technology and information security is essential in understanding how the role of information security has changed over the years. The following section describes the evolution and the change in attitude of people as organisations become more and more dependent on Information Technology.

In the early 1980s, Information Technology was commonly labeled as an unprecedented threat to the stability of employment levels in organisations (Currie, 1989, p 10). There were both optimistic and pessimistic attitudes towards Information Technology. On the one hand the introduction of new technology was seen as a way to relieve the boredom of routine jobs. This argument claimed that the new technology would enhance employees’ skills and would not be used as a tool by management to heighten its control. On the other hand, the pessimistic attitude saw technology as an unnecessary evil designed to assist management in its pursuit to decrease work and reduce the number of employees in its organisation (Currie, 1989, p 1).

Towards the end of the 1980’s, this initial ‘revolutionary’ approach to Information Technology was superseded by an ‘evolutionary’ approach which concentrated on a longer term view of organisational change (Currie, 1989, p 1). The managerial aims concerning the introduction of new technology were a reduction in operating costs, increased flexibility, improvement in quality of the product or service, and increased control and integration within the organisation (Currie, 1989, p 24).

These managerial aims assisted with the acceptance of Information Technology into organisations and computers advanced from being simple stand-alone batch applications utilised by single-users, to computers capable of multitasking and distributed processing in a distributed environment (Gerber & von Solms, 2001, p 577). The computing
environment itself has changed from a Computer-Centric environment to Information Technology-Centric and today we are in what is called the Information-Centric environment. The Computer-Centric environment was when processing operations were done in batch mode and the computer department was viewed as being important, but completely independent of other departments in the organisation. Any failures in computer operations usually had little or no effect on the behaviour of the organisation (Gerber & von Solms, 2001, p 578).

In the Information Technology-Centric era, the organisational departments began to depend a little more on the activities performed in the Information Technology department, because of activities such as real-time control and multitasking. In this environment the organisation could suffer directly if the IT department became unavailable. From the early 1990s, the Information-Centric era, the IT department started to play a vital role in the organisation. This was mainly due to the fact that information started to play such an essential part in managerial decision-making. Computers are now decisively entrenched in the structure of industry and commerce. Once looked upon with dread and misgiving, computers today are viewed matter-of-factly as useful management tools. There are two keys to effective computer use. One is managing the information. The other is ensuring that information remains secure (Information Management and Computer Security, 2001, online).

Security has evolved similarly over the years, from being focused on the protection of physical access to the computing equipment, to protecting the information in an organisation (Gerber & von Solms, 2001, p 578). As a result of this evolution, organisations were beginning to realise that Information Technology had become increasingly important in all facets of business.

Since 1994, Information Technology has emerged as a key driving force of an organisation’s decisions and strategies (King Report, 2001, p 11). As a result of this, the information possessed by an organisation is among its most valuable assets and is
essential to success. The following section will explore information security in more detail.

2.3 What is Information Security?

Since the end of the 1990’s, information has been seen as a valuable product or as a commodity (Busch-Vishniac, 2001, online). As a result of this, as with any commodity, consumers wish to have confidence in the vendor’s honesty, ability to deliver, willingness to provide service and reputation for financial stability. In other words, consumers wish to procure products based on a foundation of trust (Busch-Vishniac, 2001, online). This applies to all products and dealings, information included.

Information is defined as any type of knowledge that can be exchanged, and this information is always expressed, or represented, by some type of data (OASIS, 2002, online). Information can be found in many forms. It can be stored on computers, transmitted over networks, written down on pieces of paper or even just spoken in conversation. Computers are playing a vital role in most organisations today. Computers and computer networks form the information backbone of an organisation as they are needed to create, process and store information resources (Smith, 1989, p 193). The protection of these resources is of great importance as most organisations rely principally on information. All this information and the supporting processes are important business assets (BS 7799-1, 1999, p 1).

Commercial organisations and governments rely heavily on information to conduct their daily activities. Therefore, the security of the information needs to be managed and controlled properly (Lane, 1985, pp. 2-3; Smith, 1989, p 193). The process of protecting these organisational assets is called information security. Information security is achieved by implementing and maintaining an appropriate set of controls. This set of controls could include policies, procedures and organisational structures (BS7799-1, 1999, p 1).
2.3.1 The Importance of Information Security

Organisations rely heavily on information to perform its daily tasks. Seventy-six percent of organisations in the United Kingdom believe that they have sensitive or critical information (PriceWaterhouseCoopers, 2002, p. 3). As this information is so critical, it must be protected no matter where or how it is stored. Information security therefore needs to be implemented within the organisation to ensure that the information is kept safe and secure (Krige, 1999, p. 7).

Information security is not important for its own sake, but rather for the impact it can have on business. There is a definite return on investment (ROI) to be gained from effectively managing information security (Deloitte & Touche, 2002, online).

Information is one of the few competitive advantages left for organisations to exploit and it can cause the collapse, or at least reputational damage, to those organisations that get it ‘wrong’ (Msomi, 1999, online; Deloitte & Touch, 2002, online). However, while the importance of Information Technology itself is understood, and a high level of importance is given to managing an organisation's IT assets, the same awareness is not afforded to information security (Msomi, 1999, online).

The successful operation of organisations today depends on information and the exchange of information. However, threats to its confidentiality, integrity and availability are plentiful. Organisations are realising, more and more, that its information is a crucial asset to its way of doing business and should be looked upon in much the same way as stock, finance and buildings (Deloitte & Touche, 2002, online).

Information assets are often exposed to vulnerabilities while routine activities are being conducted. The Carnegie Mellon University estimates that ninety-nine percent of all reported intrusions ‘result through exploitation of known
vulnerabilities or configuration errors, [for which] countermeasures were available’ (13 April 2002, online). This shows how important it is to protect the vulnerabilities of the assets of an organisation. As information is such an essential asset, information security needs to be implemented to guarantee that this asset is protected satisfactorily and at all times (Krige, 1999, p 6).

The consequences for an organisation’s financial health and reputation can be devastating if information held by them were to be accidentally or deliberately disclosed to the wrong people, falsified or corrupted or rendered unavailable for a period of time (Gordon, 2002, online). All these consequences would mean that there would have been a loss of confidentiality, integrity and availability. The following subsection deals with the effects that poor information security practices could have on an organisation.

### 2.3.2 Effects of Inadequate Information Security

Protecting information in any organisation is of vital importance. In an interview with the Sunday Times, Frank Rizzo, a partner at KPMG Information Risk Management, said that while the cost of the hardware in information systems is a concern, it is the unqualified value of the information residing on the hardware that should be of greatest concern (Msomi, 1999, online).

It is difficult to gauge the exact value of the information that an organisation possesses, but it is apparent that any breach in the confidentiality, integrity or availability of information would result in devastating consequences for an organisation. Unauthorised information access places an organisation at enormous risk (Gordon and Glickson LLC, 2001, online). Information security breaches cost millions of dollars in lost business revenue. Breaches can also cause damage to reputation, lead to share price depreciation and loss in customer confidence (Zylt, 2001, online). One of the first effects would be that the organisation risks a public relations nightmare, the consequences of which can be destructive. For example, CD Universe was almost put out of business when
thousands of its customers’ credit card numbers were stolen from one of the organisation’s databases and posted on the Internet (Gordon and Glickson LLC, 2001, online).

In a recent survey conducted by Gordon and Glickson, less than four in ten consumers believe that organisations handle the personal information they collect ‘properly and confidentially’. This perception, true or not, could dissuade consumers unless an organisation has proper information security processes in place (2001, online).

Inadequate levels of information security could lead to the corruption of an organisation’s computer systems (Gordon and Glickson LLC, 2001, online). The arrival of the Internet brought about easier ways of altering, modifying and stealing information that previously had been difficult for unauthorised parties to do (Zylt, 2001, online). Hackers can read e-mails, sniff for super-user accounts and passwords and gain root or administrative access to certain machines. There are laws such as the Electronic Communications Privacy Act, the Computer Fraud and Abuse Act and the Economic Espionage Act that outlaw computer breaches, network abuse and the leaking of confidential information, amongst other issues. However, the criminal prosecution of the perpetrators will not compensate the organisation for what could be vast losses resulting from a destroyed or corrupted computer system (Gordon and Glickson LLC, 2001, online).

Therefore, the protection of information of an organisation will ultimately lead to the protection of the organisation itself (Gordon and Glickson LLC, 2001, online). An aspect of protection that must be considered is that security breaches do not just occur from external sources. Many security incidents occur within an organisation due to careless internal security or because organisations have the incorrect impression that all members of staff are performing their functions in an authorised manner (Zylt, 2001, online).
Thus, the protection of information, both internally and externally, is vital to an organisation. One of the best ways to protect information is to ensure that the three main pillars of information security are kept in place.

### 2.4 Essential Pillars of Information Security

There are three so-called pillars of information security; namely confidentiality, integrity and availability that are essential to ensuring the effective protection of information (British Standards Institute, 1999, p 1). Each of these pillars will be discussed briefly in the following subsection.

#### Confidentiality

*Can you keep a secret?*

The first pillar, confidentiality, is concerned with ensuring that information of a specific classification is not distributed to persons outside the category for which it is classified. It ensures that only those individuals who have access permissions will be able to view certain information. The category for which the information is classified could be a specific organisation, department or a definite individual. Confidentiality means that sensitive information must be prevented from being disclosed to unauthorised parties. There are generally two ways, or a combination of these, through which confidentiality can be provided. One way is to limit access to the information that must be kept secret. The other way is to encrypt the secret information. Confidentiality is sometimes also referred to as secrecy (Krige, 1999, p 8; Bruce & Dempsey, 1997, pp. 36-37).

#### Integrity

*Was the information sent correctly?*

The second pillar is integrity of the information. This is concerned with the quality and reliability of information; such that management can be assured that the information on which decisions are based has not been modified dishonestly or otherwise when the data is transferred, captured and stored. One way of providing integrity is to attach a special indicator or message digest at the end of
the message that is going to be sent. If this digest remains intact during transit then the integrity has been preserved. Integrity means that an asset or information can only be modified by authorised parties or only in authorised ways (Krige, 1999, p 9; Bruce & Dempsey, 1997, p 37).

**Availability**

*Can I get what I require when I require it?*

The third pillar is the availability of the information. Availability is concerned with guaranteeing the availability of systems and data on a timely basis so that strategic and business decisions can be effected as rapidly as possible. In the event that systems or data are unavailable, opportunities may be lost, deadlines missed or commitments defaulted. Work progress could be impaired if the information is not available when it is required. Even if the information is exactly what is needed to meet business requirements, if it is not available when needed to complete a task, it becomes useless (Bruce & Dempsey, 1997, p 41).

Confidentiality, integrity and availability are widely recognised as the three vital pillars of information security. Without adequate protection in place to prevent illegal activities, an organisation’s most important asset, namely its information, is at risk. Therefore it is critical that this asset be protected and secured through these three pillars. There are additional support structures of information security that could be used in conjunction with the three main pillars to complement them, namely; identification and authentication, access control/authentication and non-repudiation.

Information security is extremely important to the well-being of any organisation and, thus, it is essential to ensure the pillars of confidentiality, integrity and availability. There are, however, many problems or false perceptions encountered when ensuring that information security is a part of an organisation. The following section provides an overview of the problems faced when dealing with information security.
2.5 Problems with Information Security

A quote from a Deloitte & Touche booklet sums up one of the key problems with information security. They say that ‘Information security requires a whole-hearted organisational commitment of resources (financial, human and technological) to an enterprise-wide program designed to evolve and adapt to new dangers. But most people are looking for a quick fix’ (2002, online).

The vision of all organisations should be to attain a satisfactory level of information security that is sustainable. One hundred percent security should never be the goal, as failure is a certainty (Deloitte & Touche, 2002, online). Achieving security, however, includes more than just applying ‘quick fixes’. A ‘once-off’ vulnerability assessment is useful in giving an overall picture of the current state, but this assessment should be done on a regular basis. Only by addressing all facets and measuring an organisation’s performance can you accomplish sustainability of security. Even by doing this, though, physical and technical controls are tangible and can be enforced, but it is the operational controls and the associated actions and behaviour of employees that can sustain information security practices (Deloitte & Touche, 2002, online).

2.6 Conclusion

Information is a key asset for most organisations and because an organisation’s welfare depends, to a large extent, on information, it is imperative that the information be protected using information security practices. This chapter explored the background of information security and the destructive effect of poor information security in an organisation. The value of information to an organisation has been stressed and the need to protect this information with the three pillars of information security, namely; confidentiality, integrity and availability has also been highlighted. All these pillars contribute to the protection of this important asset. The relevant problems experienced with information security were also briefly explored.

The subsequent chapter will investigate the field of corporate governance. The King Report on corporate governance will be explored as a document relevant to corporate
governance in South Africa, as well as the relevant pillars that make corporate governance so important in the business world. The evolution and importance of corporate governance will be explored as well as the recommended structure of an organisation. The role that senior management plays in the overall management of an organisation will also be explored, as well as the relationship that the Board of Directors has with various parties in the organisation.
3.1 Introduction

Judge Mervyn E. King, in a presentation entitled ‘Corporate Governance: Implications for Executives’, stated that when an organisation is created it becomes a citizen of the country in which it is established. This organisation is an inanimate object until the organisation’s directors are appointed. Judge King went on to explain the awesome responsibility that these directors have towards both the organisation and the shareholders (Personal communication, August 6, 2002). This responsibility has evolved over time and has changed the role of directing an organisation. This changed role will be the focus of this chapter.

Good corporate governance practices ensure responsibility for corporate entities (Blackwell Publishers, 2000, online). This chapter will initially discuss the documentation most used in South Africa with regard to corporate governance and
corporate governance in terms of its importance to organisations will also be highlighted. Threats that might influence good management of organisations will be explored as well as the four pillars that are needed to ensure valuable corporate governance in an organisation. The chapter will conclude by investigating the structure of corporate governance.

3.2 King Report on Corporate Governance

Corporate governance is extremely important for the management of any organisation. Various reports on corporate governance, for example, the King and Cadbury Reports, have been published in this regard. This section will examine the documentation most used in South Africa with regard to corporate governance.

Corporate governance in South Africa was formalised into business practices with the publication of the ‘King Report on Corporate Governance’ in November 1994. The aim of the King Report is to ‘promote the highest standards of corporate governance in South Africa’ (King Report, 2001, p 8). The first King Report, when published, was recognised internationally as the most complete publication on the inclusive approach to corporate governance (Institute of Directors in Southern Africa, 2002, online).

The King Committee on Corporate Governance was formed in 1992, with the support of the Institute of Directors. This committee was to consider corporate governance in the South African context and how South Africa coincided with the rest of the world (King Report, 2001, p 8). The King II Report on Corporate Governance was released in 2002 and it has numerous updates on issues that have altered since 1994, for example, Information Technology (King Report, 2001, p 87). It must be noted that both the King and King II Reports are not legally binding, but rather act as principles to guide and assist senior management. The status of the King Report can thus be seen as nothing more than a code of good practice.

An additional international report regarding corporate governance is the Cadbury Report. The Cadbury Report was released in the United Kingdom in December 1992. The main
recommendation of the committee who created the report, was that the Board of all organisations registered in the UK should meet the terms of a specified code of practice and state in their financial records whether the organisation has complied and also state those areas where they have not complied, where applicable (Xrefer, 2000, online). Further international documents concerning corporate governance include the Greenbury Report from the United Kingdom, the Danish Corporate Governance Network (DCGN) and the Corporate Governance Initiative for Bulgaria. All of these reports share common aspects regarding good governance. These essential components of corporate governance will be discussed next.

3.3 Corporate Governance

Tomorrow’s Organisation and Pauffley state in ‘The Corporate Reporting Jigsaw’ that ‘If you are looking for signs that governance is working, look for clear purpose, inspiring vision, shared values, robust relationships, reciprocal accountability and balanced measurement’ (King Report, 2001, p 74).

Corporate governance is one of the decisive issues in business today. Corporate governance may have different meanings for different parties. For organisations it could mean securing access to capital. For investors, good governance could mean enhanced shareowner value (Gaines, 2002, online). This section will describe the importance of corporate governance and the underlying pillars required to ensure effective corporate governance, thereby gaining a better understanding of this field.

According to Bob Garratt, author of ‘The Fish Rots from the Head’, corporate governance indicates that Boards of Directors must lead its organisation through ‘direction giving’ and strategy implementation. Senior management is there to manage the organisation in its day-to-day operations (Planting, 2001, online). Sir Adrian Cadbury, in the foreword of Corporate Governance: A Framework for Implementation, provided a definition of corporate governance. He states that corporate governance deals with establishing a balance between economic and social goals and between individual and communal goals.
The framework for governance is there to promote the competent use of resources and, in the same way, it must involve accountability for the stewardship of those resources (World Bank Group, 1999, online). However, corporate governance has not always been the focus of the Board of Directors and senior management of organisations.

The focus of management has changed over the years. The nineteenth century saw the groundwork laid for modern corporations and was called the century of the entrepreneur. A fixation with management developed in the twentieth century and it became known as the century of management. In this century, there was the rapid growth of management theories and management teachings. It is only now in the twenty-first century that the focus of management has shifted to the legitimacy and effectiveness of the management of the organisation and guarantees to be the century of governance (King Report, 2001, p 17).

There are a number of challenges associated with good governance. One of the challenges of good corporate citizenship is to achieve a suitable balance between performance and conformance in conducting its daily activities (King Report, 2001, p 9).

Conformance means that in meeting the requirements of corporate governance standards constraints are placed on management. The Board of Directors must balance this conformance with performance to enable the organisation to achieve financial success (King Report, 2001, p 10). The objective of corporate governance is not to constrain organisations, but rather to balance the encouragement of enterprise with accountability (World Bank Group, 1999, online). The question now arises, just how important are good corporate governance practices to an organisation?

3.3.1 Importance of Corporate Governance
Effective corporate governance is essential to any organisation. This subsection attempts to highlight how important corporate governance is, not only to the organisation, but to shareholders as well.

The importance of the good governance of organisations is encapsulated in a quote from the President of the World Bank, Jim Wolfensohn, which states that, ‘the proper governance of organisations will become as crucial to the world economy as the proper governing of countries’ (World Bank Group, 1999, online).

This statement shares the sentiment of Judge King who pointed out that the organisation is a key factor in contemporary society (King Report, 2001, p 11). In many cases, organisations are a more direct presence to many citizens than government. In the global economy there are many authorities to which an organisation can ‘escape’ to reduce labour costs or evade regulations and taxes. However, this is not the case with consumers and shareowners. For organisations, this means that they cannot avoid the undesirable results of poor governance (King Report, 2001, p 11). Thus, corporate governance is very important to consumers and shareowners as well.

First-rate corporate governance is extremely important to shareowners, as is demonstrated in a survey conducted by McKinsey & Co., released in June 2000. This survey found that more than eighty-four percent of the approximately 200 global institutional investors, showed a readiness to pay a premium for the shares of a well-governed organisation over one deemed poorly governed but with an equivalent financial record (McKinsey & Company, 2000, online). Three-quarters of these investors specified that Board practices were at least as imperative as financial performance, when assessing organisations for possible investment. This highlights that shareowners are willing to pay more for proper corporate governance.
So, by simply developing good governance practices, managers can potentially add considerable shareowner value (McKinsey & Company, 2000, online). High-quality corporate governance could prove to be a challenge, though, as there are many extenuating circumstances that contribute to the breaking down of superior management. A brief discussion of these circumstances or ‘sins’ will follow.

### 3.3.2 Corporate ‘Sins’

Tomorrow’s Organisation in the United Kingdom defined the idea of the three corporate ‘sins’. These sins are sloth, greed and fear.

Business is essentially about risk taking and managing those risks. Sloth is said to be a loss of flair or a loss of risk taking when an enterprise gives way to administration. The organisation gets ‘lazy’ and avoids the risks undertaken in the past (King Report, 2001, p 10).

Greed is the second corporate ‘sin’ and it surfaces when management makes short-term decisions. These short-term decisions have an immensely positive effect on the organisation at that point in time, but have no long-term benefits. In essence, management becomes greedy (King Report, 2001, p 10).

The final corporate ‘sin’ is fear. This is where the management of an organisation becomes submissive to the shareowners and stops taking the risks necessary in business because shareowners do not feel that these risks are justified (King Report, 2001, p 10).

Sloth, greed and fear threaten the vitality of an organisation and steps must be taken to ensure that they do not encroach or stifle a healthy business. To do this, good corporate governance practices should be in place. Good governance practices can be entrenched in an organisation by implementing the four pillars of corporate governance. These pillars will be discussed in the following subsection.
3.3.3 Essential Pillars of Corporate Governance

Corporate governance is extremely important for the operation of organisations. There are four central pillars of corporate governance recommended by the King Report, namely; accountability, responsibility, fairness and transparency (2001, p 17). These pillars are required to ensure effective corporate governance, and each of these four pillars will be discussed briefly.

Accountability

Who is answerable?

The first pillar to be discussed is accountability. Accountability ensures that individuals or groups in an organisation who make decisions and take actions on specific issues are accountable for their decisions and actions. Mechanisms must exist and be effective to allow for accountability. This provides investors with the means to question and evaluate the actions of the Board and its senior management (King Report, 2001, p 14).

However, the investor concept of being accountable to all must be rejected for the simple reason that to ask Boards to be accountable to everyone would result in their being accountable to no one. The modern approach is for a Board to identify the organisation’s shareholders and to agree to policies which determine how the link with those shareholders should be controlled in the interests of the organisation (King Report, 2001, p 8).

Responsibility

Who is the guilty party?

The next pillar to be discussed is responsibility. Responsibility, with reference to management, relates to the behaviour that allows corrective action and penalises mismanagement and misconduct. Responsible management would, when required, put in place what it would take to set the organisation on the right path. While the Board is answerable to the organisation, it must act responsively to and
with responsibility towards all shareholders of the organisation (King Report, 2001, p 14).

It is important to note the difference between accountability and responsibility. The following is an excerpt from the King II Report noting the difference - ‘One is liable to render an account when one is accountable and one is liable to be called to account when one is responsible’. This means that one can be called to explain if you are accountable for something, but corrective action can be taken against you if you are responsible for something. In corporate governance terms, one is accountable by law to the organisation if one is a director and one is responsible to the shareholders identified as relevant to the organisation (King Report, 2001, p 8).

**Transparency**

*Can outsiders see what is going on inside the organisation?*

The third essential pillar of corporate governance is transparency. Transparency is the ease with which an outsider is able to make significant assessment of an organisation’s actions, its economic fundamentals and the non-financial aspects relevant to that business. This is a measure of how good management is at making necessary information available in an open, precise and timely manner – not only the audit data but also general reports and press releases. Transparency reflects whether investors obtain a correct picture of what is happening inside the organisation (King Report, 2001, p 13).

Transparency is significant both nationally and internationally. In a report by a French bank, Credit Lyonnais, South Africa ranked among the top five of twenty-five emerging nations in terms of corporate governance. However, South Africa rated poorly in terms of transparency (CLSA Emerging Markets, 2000, online). South Africa must clearly exhibit not only in theory, but in practice, flawless governance standards in all areas of commercial activity if it is to continue being a
destination of choice for up-and-coming global investors (King Report, 2001, p 12).

**Fairness**

*Is everyone treated fairly?*

The final essential pillar of corporate governance is fairness. Fairness must be in practice to ensure balance in the organisation. The systems within the organisation must be in balance to take into account all those who have an interest in the organisation. The rights of various groups have to be recognised and valued. For example, minority shareowner interests must receive equal consideration to those of the dominant shareowners (King Report, 2001, p 14).

These four pillars contribute to the overall goal of proper corporate governance. Corporate governance is fundamentally about leadership. Leadership must be efficient so that organisations can compete successfully in the global economy. The leaders of an organisation must have integrity because shareowners require the confidence and assurance that the management of a organisation will act honestly. The concepts of transparency and accountability are important to shareowners (King Report, 2001, p 22).

Leadership needs to be both transparent and accountable because otherwise business leaders cannot be trusted and this will lead to the decline of organisations and the ultimate demise of a country’s economy (King Report, 2001, p 22). The four pillars discussed are the essential pillars that should be in place according to the King Report. The King Report also recommends that three additional pillars or characteristics should, at least, be considered by an organisation.

### 3.3.4 Supporting Pillars of Corporate Governance

The four pillars of corporate governance go a long way to ensuring that good corporate governance practices are in place in an organisation. There are three
supporting pillars which help sustain these four main pillars. A short description of each supporting pillar follows.

**Discipline**
The first supporting pillar is discipline. Corporate discipline is the obligation from senior management to adhere to the conduct that is collectively identified as being acceptable (King Report, 2001, p 13).

**Independence**
The second supporting pillar is independence. Independence ensures that the decisions that are made in the organisation and any internal controls or processes that are established, are objective and that they avoid any conflicts of interest, such as supremacy by a large shareowner or the Chief Executive Officer of an organisation (King Report, 2001, p 13).

**Social responsibility**
The last supporting pillar, social responsibility, means that an organisation must be aware of social issues, especially ethical standards. By taking social factors into account, an organisation is expected to experience indirect economic benefits, such as enhanced efficiency and corporate status (King Report, 2001, p 14).

The four key pillars of corporate governance, namely; accountability, responsibility, fairness and transparency, are important for ensuring superior corporate governance, as pointed out in the previous section. Management of any organisation should also take note of the three supporting pillars of corporate governance, namely; discipline, independence and social responsibility. It is important that these pillars are addressed in an organisation through a proper structure of corporate governance.

### 3.4 The Structure of Corporate Governance
The previous section described the four pillars of corporate governance, why these pillars are central to effective corporate governance and how they should be sustained by the three supporting pillars. Although these pillars are essential for providing the framework for good corporate governance, an established structure in the organisation is also needed. This structure of corporate governance will be discussed in this section, detailing what the hierarchies in most organisations are.

3.4.1 Board of Directors

The organisation is run by a Board, which consists of the chairperson, managing director, executive directors and non-executive directors. This is the Board structure most used in South Africa (King Report, 2001, p 45). The Board must determine the organisation’s vision and values, together with the strategy that is to be used to achieve this vision. The Board has a primary duty to exercise its fiduciary responsibility in the best interests of the organisation and its stakeholders (TIAA-CREF, 1998, online). Another important function of the Board is to guarantee that procedures and practices are in place to protect the organisation’s assets, as well as its reputation (King Report, 2001, p 45). Furthermore, the Board of Directors must supervise and evaluate the implementation of strategies, policies and business plans in the organisation. In addition, it is extremely important for the Board to ensure that the organisation acts in accordance with relevant laws, regulations and codes of practice that apply to that organisation (King Report, 2001, p 46).

3.4.2 Chairperson

There should be a very clear division of responsibilities at the head of the organisation, which will help to ensure a balance of power and influence so that a single person will not be able to make unregulated decisions (King Report, 2001, p 52). The Board is subject to the firm and objective leadership of a chairperson. The most important function of the chairperson is to supervise meetings of directors and to ensure the smooth functioning of the Board in the interests of good governance. The chairperson will also preside over the organisation’s
shareowners’ meetings and acts as the informal link between the Board and senior management and between the Board and the Chief Executive Officer (CEO) (King Report, 2001, p 51).

### 3.4.3 Chief Executive Officer

The Chief Executive Officer (CEO) has a very significant and strategic role to play in the success of an organisation. The role that the CEO should play is to recommend to the Board a durable vision for the organisation that will create agreeable levels of shareowner value and good relations with other shareholders. The CEO must also devise and oversee the implementation of key management policies (King Report, 2001, p 53).

The evaluation of an organisation’s CEO is a vital Board responsibility. A clear understanding between the Board and the CEO regarding the organisation’s expected performance and how that performance will be measured is very important. A high standard of accountability and ethical behaviour should be set at the top of the organisation (TIAA-CREF, 1998, online).

### 3.4.4 Directors

All directors, whether executive or non-executive, are bound by their fiduciary duties to the organisation. The person/people who own property (i.e. organisation) delegates unlimited management power to another person (i.e. directors of an organisation). It is then the fiduciary duty of the directors to act with the greatest trustworthiness in the position given to them. An executive director is involved in the everyday management and could be in the full-time employment of the organisation (King Report, 2001, p 60). A non-executive director is not involved in the everyday management and is not a paid employee of the organisation (King Report, 2001, p 56).

In addition to the executive and non-executive directors, there is the independent director. The independent director is a non-executive director who has no
business relationship with the organisation, or any other relationship which could be seen to compromise their ability to make independent decisions. The Board has a joint responsibility to provide effective corporate governance, which involves a set of relationships between the senior management of the organisation, its Board and its shareholders (King Report, 2001, pp. 56-57).

The duty of the senior management or directors is to give effect to the policy prescribed by the Board and to attend to the daily conduct and administration of the business of the organisation (Leveson, 1970, p 52).

3.4.5 Shareholders
Shareholders are identified as any person, entity or interest group that has some relationship with an organisation. There are three types of shareholders, namely; shareowners, contractual shareholders and non-contractual shareholders. Shareowners are those individuals who own stock directly, through mutual funds (New York Stock Exchange, 2001, online). Contractual shareholders are those shareholders that have contractual relationships with the organisation. These could include customers, employees and suppliers. Non-contractual shareholders are those shareholders that have a relationship with the organisation that does exist because of contracts. These could include neighbours, government and local authorities.

Communication between the shareholders and the Board of Directors is a very important feature of corporate governance. The Board has the duty of presenting a balanced assessment of the organisation to the shareholders, which includes both the positive and negative aspects of the organisation (BDO, 1999, online).

All these parties should work together to create a harmonious environment in organisations. To address some of the most important areas of fiduciary responsibility, all these parties should cultivate and encourage a corporate environment of sturdy internal controls, accountability, high ethical standards and compliance with relevant
laws and regulations (TIAA-CREF, 1998, online). As seen from the discussion above, the Board of Directors is responsible for overseeing the management of an organisation, whereas senior management is responsible for the implementation of policies and procedures and the daily running of an organisation. The Board, chairperson, CEO, directors and shareholders all play an important role in creating an effective chain of corporate governance.

3.5 Conclusion

This chapter explored the field of corporate governance. The King Report on Corporate Governance was highlighted, as well as other international committees that have investigated corporate governance. The considerable importance of corporate governance and the threats to this field have also been discussed, as well as the four essential pillars required for the effective management of an organisation. The three supporting pillars were also discussed, together with the structure of corporate governance. The structure detailed the various roles that are played by members of the Board of Directors and senior management and the duties that should be fulfilled by them.

As has been stated in this chapter, corporate governance is there to promote the competent use of resources and it must involve accountability for the management of those resources. Effective corporate governance practices should be used by all parties in an organisation to create a structured and harmonious environment in which to work. When following effective corporate governance practices, one of the main functions of the Board of Directors is to ensure that various practices and procedures are in place to protect the organisation’s assets and resources. Senior management, using proper corporate governance practices, must ensure that these policies and procedures of the Board are effectively implemented in its organisation. This function of senior management to protect assets and implement policies will
be discussed in Chapter 5, and the relationship between corporate governance and information security will be investigated.

The following chapter will take an in depth look at the field of corporate culture. The term ‘culture’ will be examined, as well as how a corporate culture develops. The levels of corporate culture, as defined by Edgar H. Schein, will be explored and the functions of a culture in an organisation will be studied. And just as the importance of corporate governance to an organisation was detailed in this chapter, the following chapter will highlight the importance of corporate culture to an organisation.
Chapter 4: Corporate Culture

4.1 Introduction

The previous chapter explored the concept of corporate governance and who should be responsible for the managing of an organisation. The vital responsibility that senior management has to the organisation was explored, as well as the importance of the pillars of corporate governance. Effective corporate governance is essential to an organisation. Another aspect that is important as far as the success of an organisation is concerned, is that of corporate culture.

This chapter will explore the various facets of corporate culture. Various definitions of culture and the beginnings of culture will be explored. The three levels of culture, the
numerous types of culture that exist and the functions of a culture will also be looked at in detail.

4.2 What is Corporate Culture?

Organisations develop cultures whether they try to or not. The culture of an organisation operates at both a conscious and unconscious level and if management does not understand the culture in its organisation, it could prove to be fatal in today’s business world (Hagberg Consulting Group, 2002, online).

Every organisation has a culture and this culture could be operating in one of two ways. It could be operating with authoritative principles and driven by top management. On the other hand, many organisations have a culture that exists by default. This culture changes by accident and is influenced by a few key people in the organisation (Atkinson, 1997, p 16). A disturbing fact is that it is estimated that only five percent of organisations have a definable culture, where senior management takes an active role in the shaping of the culture (Atkinson, 1997, p 17).

Cultural assumptions in organisations develop around how people in the organisation relate to one another, but that is only a tiny proportion of what culture covers (Schein, 1999, p 28). Corporate culture is generally defined as values that are shared by everyone in an organisation, including fundamental beliefs, principles and practices (Beveridge, 1997, online). Culture is the sum total of all the shared, taken-for-granted assumptions that a group has learned throughout history. Cultural assumptions involve the internal workings of an organisation as well as how an organisation views itself in relation to its various environments (Schein, 1999, p 29). Culture is shared, and because it lies at the heart of what employees do and think, the organisation’s culture provides these employees with a common belief that binds them together as a group (Sathe, 1983, pp. 6-7).

According to Edgar H. Schein, the biggest risk in working with culture is to oversimplify it and miss several basic facets that matter. These facets include:
Corporate culture is deep. Culture controls the employees more than they control the culture. Culture gives meaning and predictability to the daily organisational life. As the employees learn what works, they develop beliefs and assumptions that eventually phase out of their conscious thinking and become tacit rules of how things are done (1999, p 25).

Corporate culture is broad. As a group learns to survive in its environment, it learns about all aspects of its external and internal relationships. If there is no specific focus for wanting to understand the organisational culture, it will seem endless and frustrating (1999, p 26).

Corporate culture is stable. The employees in an organisation or the members of a group want to retain their cultural assumptions as the organisational culture provides meaning and makes work situations predictable. Therefore, culture is one of the most stable parts of an organisation (1999, p 26).

Corporate culture is an extensive issue and because the shared beliefs of an organisation include values about what is desirable and undesirable – how things should and should not be – these beliefs dictate the kinds of activities that are ‘legal’ and the kinds that are ‘illegal’ in an organisation (Beyer, 1981, p 21).

As has been seen, culture has depth, is far-reaching and is one of the most stable aspects of an organisation, and consequently, a culture does not develop overnight. The following section explains how a culture begins and is formed over time.

### 4.3 The Origins of a Culture

The activities of a group are governed by formal and informal rules. These rules start to take on a life of their own and may begin as straightforward statements about the activities of group members, but they evolve into something more complicated. In other words, the purpose and activities that typify the group in its formative years give way to
more sophisticated concepts. Together with this change comes a sense of group identity and the beginnings of a culture (Beach, 1993, p 16).

The activities of a group or organisation contribute to the growing culture and consequently, the culture begins to influence the activities by determining which activities are acceptable and which are not (Beach, 1993, p 17). Thus the culture not only places limitations on the activities of an organisation and its employees, it also prescribes what an organisation and its employees must do. The culture, therefore, guides the activities of an organisation and its employees (Beach, 1993, p 11). A mutual relationship develops between activities and culture, each influencing the other (Beach, 1993, p 17).

As an organisation grows, the relationship between its activities and its culture becomes more complex. A sense of direction or an agenda begins to develop. This agenda that the organisation perceives itself to be pursuing is its vision (Beach, 1993, p 49).

Activities, culture and vision become an interconnected whole. The culture of an organisation represents its primary beliefs and the imperatives that are dictated by these beliefs. Activities result from these imperatives, but they also influence the beliefs themselves. Vision defines the perfect future; possibly advocating the current culture or suggesting change (Beach, 1993, p 50).

Therefore, it is the formative activities and the vision of an organisation that lead to the origins of the organisational culture. Once the culture is established, however, the culture influences the activities of an organisation. Whether a culture is effective and whether it should be changed or not, the various levels of culture need to be addressed. The following section will detail the various levels of culture that exist.

4.4 Three Levels of Culture

One of the problems when trying to understand culture is to oversimplify this complex field. It is very simple to say that culture ‘is the way things are done around here’, but a
far better way of thinking is to realise that culture exists at several levels. These levels range from the very visible to the tacit and invisible. Furthermore, it is imperative that these levels are managed and understood (Schein, 1999, p 15). The following subsection addresses this issue of culture existing at numerous levels.

4.4.1 Level 1: Artifacts

The first and easiest level of culture to observe in an organisation is that of artifacts (Hagberg Consulting Group, 2002, online). Artifacts can be described as what an individual can see, hear and feel as they observe an organisation (Schein, 1999, p 15). These include the architecture and decor, the clothing people wear and organisational processes. Other tangible expressions of culture are found in commonly used language and jargon, logos, brochures and organisation slogans. An outsider can often spot these artifacts upon entering an organisation. For employees, however, these artifacts have often become part of their unconscious thinking (Hagberg Consulting Group, 2002, online).

It is not, however, reliable to base the judgment of an organisation’s culture on simply observing the artifacts. By doing this, all that is known for sure is that the organisation has particular ways of presenting itself and dealing with customers and employees. It is still unclear at to what all these observations mean (Schein, 1999, pp. 15-16). In other words, at the level of artifacts, the corporate culture is very clear and has an immediate emotional impact. The behaviour of individuals is very clear, but it still is not clear as to why the employees of an organisation behave in a certain way and why each organisation is constructed as it is.

The observations of the actions and behaviour of individuals must now be further explored by talking to employees to attempt to gain an understanding of their perceptions about the artifacts and culture. The questioning of the employees in this regard leads to the next level of culture (Schein, 1999, pp. 16-17).
4.4.2 Level 2: Espoused Values

The second level of culture is the espoused values of an organisation. This level of culture requires questions to be asked about the organisation’s artifacts, especially those artifacts that seem somehow inconsistent with what would be expected. For this purpose, employees who can explain the organisation need to be found. Anthropologists call these employees ‘informants’ and depend heavily on such conversations to understand what is going on. The espoused values of an organisation should reflect the vision for the organisation and are those values that an organisation is said to be promoting. Examples of espoused values are teamwork and good communication (Schein, 1999, p 17).

In many cases organisations that advocate the same values can have very different physical layouts and working styles. When it comes to espoused values, organisations cannot be slotted into a specific ‘typology’ as these organisations are still not understood at the deeper cultural level (Schein, 1999, p 17).

There could be obvious inconsistencies between some of the espoused values and the visible behaviour of an organisation. Organisations may espouse teamwork, yet seem to reward and promote initiatives that are highly competitive and individualistic. An organisation may also espouse customer orientation and yet does not employ people who seem very polite or service-oriented (Schein, 1999, p 18).

What these inconsistencies indicate is that a deeper level of thought and perception is driving the obvious behaviour (Schein, 1999, p 18). What an organisation strives to do and the values it hopes to endorse may be different from the values, beliefs, and norms expressed in the actual practices and behaviour of the organisation (Hagberg Consulting Group, 2002, online). The deeper level may or may not be consistent with the values and principles that are espoused by the organisation. To truly understand the culture of an organisation one must understand what is happening at the deeper level (Schein, 1999, pp. 18-19).
4.4.3 Level 3: Shared Tacit Assumptions

To understand the deepest level of culture, the history of an organisation needs to be examined. What were the values and beliefs of the key leaders that made it successful? Organisations are started by individuals or small teams who originally impress their own beliefs, values and assumptions on the people whom they hire. If these values and beliefs of the key leaders are not in agreement with what the environment of the organisation allows, then the organisation fails and never cultivates a culture in the first place. If these beliefs and values lead to the successful creation of products and success in the chosen environment, then these values eventually become shared and taken for granted. They become tacit assumptions about the nature of the organisation’s environment and how to succeed in it (Schein, 1999, p 19).

In other words, the core of corporate culture is these mutually learned values, beliefs and assumptions that become taken for granted as the organisation continues to be successful. Originally, these values were abstract thoughts of the founders and leaders of the organisation, but they became shared and taken for granted only as the new members of the organisation realise that the beliefs, values and assumptions of their founders led to organisational success and so must be ‘right’. For these assumptions to become the corporate culture they must result from a joint learning process (Schein, 1999, p 20).

After examining the three levels of culture, it is evident that it is the learned, shared tacit assumptions on which people base their daily behaviour (Schein, 1999, p 24). From this it can also be seen that several of the most important elements of culture are essentially invisible (Schein, 1999, p 21). It is essential that the levels of culture are recognised and explored in detail to fully appreciate the depth of culture. Once an understanding of the various levels of culture has been gained, an organisation’s culture can be typified by examining the various types of culture.
4.5 Types of Culture

When an organisation is first started, it can be described as a group of people with a common purpose. There is a unique culture that is necessary for the group to survive and progress. As the group evolves, the original culture that served all of the members in earlier times becomes less practical as the group becomes an organisation (Beach, 1993, p 18). The culture will develop into one of the types of culture that have been identified. Two common types of culture, either unified or fragmented, will be discussed together with the subcultures that exist in both of these types.

4.5.1 Subcultures

No matter how pervasive a culture is thought to be, it cannot be wholly homogenous. Subcultures exist in any culture and each division or unit in the organisation sees things from a slightly different perspective. These subcultures contribute to the two types of culture; unified and fragmented. Whether a unified or fragmented culture is good or bad depends on the circumstances and the organisation’s goals (Beach, 1993, p 20).

4.5.2 Unified Culture

The first type of culture is the unified culture. The overlap among the subcultures is the organisation’s overall, unified culture. This overarching culture is not necessarily distributed at the top of the organisation to filter down to the lower levels. Management may think that this is the case and that if it changes the culture from the top that it necessarily will change throughout the organisation. This in fact is not always the case. It is much more difficult to change a culture. The reason for this is that the culture is embedded throughout the organisation as part of each subculture and it takes a major effort to change each of those subcultures (Beach, 1993, p 18).

A unified culture, however, is not always the best culture for an organisation. If every person in the organisation sees things in the same way because they share the same set of beliefs, the organisation may become immensely rigid. In a
unified culture, the leadership may have difficulty instituting change and an organisation often lacks creative ways of coping with unfamiliar threats and crises (Beach, 1993, p 19).

### 4.5.3 Fragmented Culture

The second type of culture is the fragmented culture, found in many organisations. The subcultures in an organisation do not always share much common ground. If this is the case, it is called a fragmented or weak culture. Here each subculture is substantially different, which is not always bad. For this type of culture to succeed, the organisation needs to be under good leadership, as it is the role of management to hold these various subcultures together (Beach, 1993, p 19).

However, there are many drawbacks to a fragmented culture being present in an organisation. A fragmented culture is frequently an indication that an organisation is disintegrating – its various units each fending for themselves without any concept of shared dependency and the togetherness that cooperation and community can generate (Beach, 1993, pp. 19-20).

The type of culture displayed by an organisation is largely dependent on the environment in which it operates, and what works for one organisation, in terms of culture, may not work for another. Regardless of whether an organisation’s culture can be defined as unified or fragmented, it can be identified by one of the four cultural variants, namely; role, task, power or person culture.

### 4.5.4 Role Culture

The role culture is the first cultural variant and it is possibly the most recognised and common of all the cultural types. It is based on the role that a person plays rather than an individual’s personality. It is characterised by the traditional hierarchical structure. The strengths of the role culture are in the predictability and stability of the daily routine. The role culture’s weaknesses mirror its
strengths. The weaknesses are the inflexibility and slowness of reaction in the daily practices (Handy, 1991, online).

The rigidity of this type of organisational culture can cause problems as the structure can develop an environment where employees have a narrow-minded view of their jobs (Handy, 1991, online). The focus of the role culture tends to be impersonal and it suppresses individual attempts at system improvements (Handy, 1991, online).

4.5.5 Task Culture
The task culture is the second variant and it is the culture where management is principally focused on the permanent and successful solution to problems. Performance is reviewed in terms of problems solved and the resulting effects. The task culture operates within a structure; however, it is flexible and capable of being transformed depending upon the current task (Handy, 1991, online). The organisation is consequently more loosely bound than the role culture. Power and respect come from individual knowledge rather than rank or position and the power that is being exhibited depends on the current task (Handy, 1991, online).

4.5.6 Power Culture
The third variant is the power culture. This culture tends to rely on a central figure for its strength and the lines of communication branch out from these. Because of this principal power, the structure of the culture is one where it is able to move quickly and respond to change and external threats (Handy, 1991, online).

The power culture is most often found in small organisations, but this culture frequently evolves as the organisation grows, as this power is difficult to maintain. Politics is important in an organisation with this cultural variant and the ability to anticipate the actions of the central figure is crucial for survival.
Therefore, this culture is able to exercise strict internal control. It is often a case of conform to the culture or leave the organisation (Handy, 1991, online).

4.5.7 Person or Star Culture

The last cultural variant is the person or star culture. This culture focuses solely on the individual. Although this is not a common culture on which an entire organisation should be based, it is found in small areas of large organisations. The culture is that of educated individuals, specialists in their field, who have come together because of a common interest. These individuals feel that they know what is best for an organisation and continue in their ways regardless of the overall corporate culture (Handy, 1991, online).

Elements of more than one culture may be evident in an organisation. Every organisation has a culture, which functions at both a conscious and unconscious level. To fully understand the deeper facets of corporate culture, the various levels of culture need to be explored and recognised, as well as the many types of culture that could exist in organisations. Now that these aspects of culture have been investigated, the question that remains is: what exactly does corporate culture do and what effect does it have on an organisation?

4.6 Functions of Corporate Culture

Corporate culture is deep, broad and one of the most stable parts in any organisation. It exists in levels and an organisation’s culture has, at least, seven important functions in the general running of the organisation (Beach, 1993, p 12). This section details these functions of corporate culture.

- The first identifiable function of corporate culture is that it details what is of key importance to an organisation. The standards against which an organisation’s successes and failures should be measured are also identified by the corporate culture.
The second function of culture is that it dictates how the organisation’s resources should to be used and what they should be used for.

The third function of corporate culture is that it establishes what the employees of an organisation should expect from one another in their daily behaviour.

The fourth function of corporate culture is that it produces techniques of controlling behaviour within the organisation that are legitimate and makes other techniques or methods illegitimate. In other words, the culture classifies where the power lies within the organisation and how this power is to be used.

The fifth function of culture is where it indicates the behaviour that the employees of an organisation should or should not participate in and how this behaviour should be rewarded or reprimanded.

The sixth function of corporate culture is that it determines how fellow employees should be treated and how customers should be treated. In dealing with customers, the behaviour of employees could range from being collaborative and honest, to being distant or even hostile.

The seventh and final function of corporate culture is that culture instructs the employees of an organisation on how to deal with the external environment. The behaviour of employees in this instance could be aggressive, exploitative, responsible or proactive (Beach, 1993, p 12).

From these functions it is apparent that corporate culture plays an extremely important role in the operation of organisations.

4.7 Why Does Corporate Culture Matter?

Culture is the most important aspect of an organisation as it influences the behaviour of management and employees in an organisation (Atkinson, 1997, p 17). The corporate culture is central to restraining or enhancing the performance of an organisation (Atkinson, 1997, p 16). Culture matters because it is a powerful, underlying and often unconscious set of forces that establishes individual and group behaviour. Corporate culture matters especially because cultural elements determine the strategy and goals of an organisation (Schein, 1999, p 14).
A constructive and encouraging culture will motivate the employees to achieve their full potential, which will have a considerable impact on the organisation’s performance. A negative culture will create an environment where the employees carry out their duties because they are afraid of the consequences if they do not (Atkinson, 1997, pp. 16-17).

4.8 Conclusion
This chapter explored the field of corporate culture. A definition of corporate culture was examined, as well as how a culture comes into being. The relationship between activities, culture and vision was also investigated. The vision of an organisation outlines an idyllic future, with all parties working to the benefit of the organisation. The achievement of this vision is largely dependent on the culture which results in the activities of the employees. Thus, the activities and culture are interrelated to a large extent. The culture guides the organisation in determining what activities are allowed and what activities are not allowed by the employees of the organisation. In addition, the way in which the activities are performed influences the corporate culture.

The three levels at which culture exists were also investigated. These three levels are vital to the understanding of corporate culture, as they explain the visible behaviour of employees and where this behaviour originates. The Artifacts Level of culture displays the behaviour of employees which is directly influenced by the beliefs of the employees resulting in the Shared Tacit Assumptions Level of culture. Therefore, the behaviour of employees is directly influenced by the culture of the organisation, as it gives employees a framework in which to work. The four variants of corporate culture, proposed by Handy, were studied and these variants are important for an organisation to identify what type of culture currently exists and whether this culture is beneficial to its vision. The functions of culture in an organisation were also looked at. These functions include defining what is of importance to an organisation and producing techniques for controlling the behaviour of the employee. The culture specifies the behaviour expected from the employees and the results of not adhering to this behaviour.
From this chapter it can be concluded that the corporate culture of an organisation plays a definite role in the way the employees act and behave. Thus, the actions and behaviour of employees can be changed by transforming the corporate culture.

The following chapter will investigate the relationship that currently exists and should exist between information security and corporate governance. The role that senior management should play in determining the impact of information security in the organisation will be explored as well as the extent to which they are accountable and responsible for information security. This accountability and responsibility of senior management in terms of information security will be investigated in a later chapter together with the importance of corporate culture.
5.1 Introduction

The chapter on information security, Chapter 2, explored the value of information to an organisation and the need to protect this information from the loss of confidentiality, integrity and availability. It was concluded that information is a key asset to any organisation. The chapter on corporate governance, Chapter 3, explored the significance of this field and the threats to effective corporate governance, as well as the four essential pillars needed for the successful governance of an organisation, namely; accountability, responsibility, fairness and transparency. It was concluded from that chapter that senior management must ensure that various policies and procedures are in place to protect the assets of the organisation.
Information is a key asset to the success and well-being of an organisation. For this reason, information must be protected for the consequent protection of the organisation. As part of good corporate governance practices, senior management must ensure the well-being of the organisation. As information is an important asset to an organisation and the effective protection of this asset influences the well-being of an organisation, it follows that senior management should be ultimately accountable and/or responsible for the protection of information in the organisation. This chapter will investigate the relationship that exists between the fields of information security and corporate governance, and will attempt to define the ideal relationship that should exist between the two.

This chapter will initially describe the challenge facing the relationship between the fields, followed by an examination of risk management and the associated internal control system. The Corporate Information Security Policy will then be investigated, followed by the responsibility and accountability of senior management towards information security. The chapter will conclude with reference to some legal aspects relating to information security and how they should affect the role played by senior management.

5.2 The Challenge Facing Information Security
Managing information security has become increasingly difficult and challenging. In the past, the protection of information could be accomplished with centralised controls, now managers must monitor security at a more widely dispersed level (Krause & Tipton, 1998, online). The protection of the confidentiality, integrity and availability of information is of utmost importance. It is becoming progressively more obvious that access to correct information at the right time is imperative to gaining competitive advantage or simply remaining in business (PriceWaterhouseCoopers, 2002, p 1). Therefore, protecting information assets is an absolute must for any organisation.
An adverse perception, with both management and employees, is that information security is about protecting computers, therefore a technical issue. This is not the case; it is about the all-important asset of information. There are many issues that affect information security, and many of them do not deal with computers and networks. Information security transcends many facets of an organisation and is one of the most significant policy and structure decisions in an organisation (Spafford, 1998, online). As discussed previously, policies and procedures are the responsibility of senior management. As information security is one of the most important policy and structure decisions in an organisation, it follows that senior management should be responsible for setting strategic direction regarding the protection of information, through the Corporate Information Security Policy. The Corporate Information Security Policy will be discussed in a later section.

Information security is important to any organisation. However, according to Ian Williams, Datamonitor’s security analyst, more than fifty percent of organisations worldwide spend five percent or less of its Information Technology budget on information security. Although there is no current benchmark to indicate how much of an IT budget should be spent on information security, it is indicated that five percent is too little (13 April 2002, online). According to the PriceWaterhouseCoopers 2002 Information Security Breaches Survey, it is extremely difficult for business-minded individuals to apply normal commercial principles to information security. Only thirty percent of United Kingdom businesses evaluate the return on investment (ROI) on their information security expenditure. Therefore, it is extremely difficult for management to justify expenditure on information security. The survey also details that only twenty-seven percent of organisations in the United Kingdom spend more than one percent of their Information Technology budget on information security and only five percent of organisations spend more than ten percent (PriceWaterhouseCoopers, 2002, p 3).

These are somewhat perturbing statistics, when previous chapters in this dissertation have accentuated the importance of information to organisations. The preceding chapters have highlighted that the entire well-being of an organisation could be dependent on its
information. However, as has been seen from the statistics, the protection of this information is not given much support. The following quote supports the lack of attention that information security is receiving. ‘The root cause is that security is treated as an overhead rather than an investment’ (PriceWaterhouseCoopers, 2002, p 3). This quote implies a lack understanding of the importance of information security to an organisation. Further, the White House technology supervisor, Richard Clarke, provides the following quote on the issue of information security. He says that ‘Most organisations don’t spend as much money on protecting their data as they do on coffee for their employees’ (Wilsker, 20 June 2002, Cyber Threats, e-mail). Therefore, it can be said that the most significant problems with information security are usually not the technology issues, but the issues of awareness, education and use (Spafford, 1998, online).

One of the prevalent complaints from security professionals is related to the fact that they feel that management does not understand or properly appreciate the problems related to ensuring the protection of its information assets (Hall, 2001, online). It can thus be concluded that currently information security does not, in most cases, receive the necessary attention or understanding by senior management. This is quite worrying if it is taken into consideration how important information is to an organisation.

There are numerous challenges facing the integration of corporate governance and information security – one of which is to convince the senior management of an organisation that it is ultimately accountable and responsible for the protection of the organisation’s information. The inattentiveness of management to information security could be as a result of the fact that managers can normally only allocate a limited amount of time and consideration to information security. As a result, management’s attention is often limited to a small set of acute threats and countermeasures that relate to the issues of the day (Buren, van der Meer, Shahim, Barnhoorn & Roos Lindgreen, 1999, p 76). Further security measures are, therefore, often not heeded as management is not aware of their importance to the organisation. However, just as with the performance of financial processes, details on the performance of security processes should also be brought to the
attention of senior management in an efficient and balanced manner (Buren et al., 1999, p 76). This is to ensure that management is aware of the information security situation in their organisation, so that they can take decisive action. The 2003 CSI/FBI Computer Crime and Security Survey reports that, once more, theft and loss of proprietary information resulted in the greatest financial loss for organisations (Computer Security Institute, 2003, online). Therefore, it is once again highlighted that the protection of information is essential to the success of an organisation. Senior management is ultimately responsible for the well-being and success of the organisation and the financial loss experienced with breaches in information security will adversely affect the well-being of an organisation.

Therefore, it can be concluded that senior management is responsible for ensuring that an adequate level of information security is in place in the organisation. To protect the organisation from financial loss through breaches in information security, management must reduce the inherent risk associated with the assets in the organisation. Risk management is used to reduce risks associated with assets in an organisation and is inherently part of good corporate governance practices. For this reason it is important to investigate what risk management in the information security environment precisely entails and also to identify how senior management will accomplish this. Therefore, the next section will take an in-depth look at risk management which will be followed by how internal controls should be utilised to mitigate risk. The role of the Corporate Information Security Policy in this regard will then be highlighted.

5.3 Risk Management

One of the principal responsibilities of senior management is to guide the organisation in achieving its vision. The risks facing an organisation threaten the achievement of this vision. A risk is an uncertainty about a potential event or the possibility that a negative event is going to occur without an organisation being equipped to handle it (The Alliance, 2001, online; Medical College of Wisconsin, 2001, online). Risks, if not properly managed, could be harmful to an organisation and preventative measures should be put into place through a process called risk management. Senior management must,
according to good corporate governance principles, ensure that there is a resolute system of risk management, which is necessary to protect the organisation’s assets and to support business objectives (King Report, 2001, p 97). The following section will investigate this important component of corporate governance.

One of the main aims of risk management in an organisation is to avoid or lessen the impact of risks. The risk management process involves the planning, arranging and controlling of activities and resources to minimise the impact of all risks. This process consists of distinct steps which support better decision making by contributing to a greater understanding of risks and their impacts (Risk management – an Australian portal, 2000, online; King Report, 2001, p 97). Once risks have been identified through the risk management process, these risks must be reduced to levels that are acceptable to shareowners and other shareholders that have been identified by senior management as being relevant to the organisation (King Report, 2001, p 97).

It is senior management’s obligation to demonstrate that it has dealt comprehensively with the issue of risk management and internal control (King Report, 2001, pp. 96-97). A risk management process identifies risks threatening the assets of an organisation, while internal controls are the methods and procedures used to minimise these risks identified during the risk management process. Internal control will be discussed in a later section. While risk management practices should be followed throughout an organisation by all employees in their regular activities, it is ultimately the responsibility of senior management. As CEOs, directors and managers increasingly become personally accountable for losses, they need an approach that assures they understand the implications and risks associated with every decision they make (Risk management – an Australian portal, 2000, online). The decisions made by senior management must include those regarding information and information security. Information is regarded as an intangible asset, separate from the media on which it resides and because risk management is ultimately about protecting assets, it is important that risk management includes the protection of information (Krause & Tipton, 1998, online).
Information security risk management should be part of the overall risk management process of an organisation (Information Security Guidelines Part 1 – Risk Management, 2002, online). As mentioned earlier, information is widely dispersed in organisations and legitimate users have greater access to information than ever before. Unfortunately, greater access to information exposes organisations to a number of new threats and risks regarding the protection of their information. Therefore, organisations need a way to understand the risks to their information and, as a result, create strategies for addressing those risks. This should result in an effective information security risk management process, which is a major component of the overall information security strategy of an organisation (OCTAVE, 2003, online). Therefore, it can be concluded from this section that an effective risk management process is crucial to the sustainability of an organisation. Furthermore, an information security risk management process is a vital component of overall risk management to combat the increasing number of risks threatening the information of an organisation. There are a variety of advantages for an organisation using risk management and the following subsection will investigate the benefits of an effective risk management approach.

5.3.1 Benefits of Risk Management

Risk management is a process of controlling or reducing risk that is employed principally by the senior management of an organisation. In addition to the fact that risk management forms part of proper corporate governance, there are a number of benefits for an organisation that employs proper risk management.

Risk management assists senior management in its duties as it enables more effective and well-organised strategic planning for an organisation. It also increases shareholder value by minimising losses of an organisation and maximising the opportunities. Also, the risk management process enables an organisation to have a raised awareness and understanding of the risks inherent in the organisation (Risk management – an Australian portal, 2000, online). Together with the number of benefits provided by a risk management process, a great deal of responsibility and accountability is imposed on the organisation.
5.3.2 Responsibility and Accountability for Risk Management

Risk management is a process that needs to be performed throughout the entire organisation to assist in the protection of important assets. However, even though this process should be employed by everyone in an organisation, this process is ultimately the responsibility of senior management. To support senior management in the discharge of its duties with regard to risk management, management may appoint a risk management committee to manage the entire risk management process and the major risks that are facing the organisation. This management committee is accountable to senior management for designing, implementing and then monitoring the methods used in risk management (King Report, 2001, p 98). Therefore, it can be concluded that regardless of whether risk management is delegated or not, it is ultimately the responsibility of senior management.

Risk management is very important for the proper supervision of risk and the protection of assets in an organisation – one of the assets being information. Senior management is ultimately responsible for the risks that the organisation takes and any consequences there may be if the risks are not properly managed. Therefore, as there are many risks facing the information of an organisation, senior management should be ultimately responsible for the information security risk management in an organisation.

The mechanism for controlling or reducing risk is termed internal control, and should be used in conjunction with risk management. Internal control cannot guarantee the elimination of all risks; it simply controls unnecessary and avoidable exposure (King Report, 2001, pp 96-97). The following section investigates the importance and the types of internal control that exist.

5.4 Internal Control

Internal control is defined as a process, consisting of methods and procedures, put into practice by management intended to provide reasonable assurance towards the success of
an organisation’s vision, objectives and goals. At the same time, the internal control process is used to ensure that these goals are met in the most effective way. An internal control system comprises a number of internal controls, used to achieve the objectives of the internal control system (State of Michigan Office of Financial Management, 1999, online; Medical College of Wisconsin, 2001, online).

An overall internal control system is an integrated collection of internal controls and it contains all policies, methods and procedures that are used to achieve the five main objectives of an internal control process. These five objectives are firstly to ensure the reliability and integrity of information, secondly, to guarantee that the organisation complies with any policies, procedures or laws that are applicable to the organisation, and thirdly to protect the assets of an organisation. The fourth objective of an internal control system is the efficient use of resources and, lastly, an internal control system is used for the achievement of the organisation’s established goals (Medical College of Wisconsin, 2001, online). As detailed in Chapter 3, the achieving of goals is a main component of corporate governance and it follows that an internal control system is an important part of corporate governance, as it assists in the achievement of the organisation’s goals. Further objectives of an internal control system are to ensure reliability and integrity of information and to protect the assets of an organisation. Therefore, it can be concluded that an effective internal control system is essential in assisting senior management in the protection of information and other important assets in the organisation. For that reason, it is important to fully understand internal control systems. The following subsection outlines a few basic concepts regarding the internal control system.

5.4.1 Fundamental Concepts in an Internal Control System

To gain a better understanding of an internal control system and its use in an organisation, a few concepts addressing internal control need to be explored. This subsection deals with these concepts.

*Internal control is an ongoing process.* Internal control is not a particular event, but a sequence of activities that filters through an organisation. These activities
and actions should be inherent in the methods used by management in its day-to-day operations (State of Michigan Office of Financial Management, 1999, online).

*Internal control is affected by people.* Management is ultimately responsible for maintaining a successful internal control system. Management is able to achieve this by delegating responsibilities to all employees of an organisation. In this way, employees are able to implement the internal control system that management has put into place (State of Michigan Office of Financial Management, 1999, online).

*Internal control provides reasonable assurance not absolute assurance.* Irrespective of how well or detailed an internal control system is, it cannot provide complete assurance that goals will be met. Errors in human judgment, for example, can hinder the achievement of goals (State of Michigan Office of Financial Management, 1999, online).

It can be concluded from this subsection that an internal control system is a pervasive method for protecting assets and senior management is ultimately responsible for this valuable, but not foolproof, internal control system. These underlying concepts of internal control all aim to provide assurance that objectives can be achieved. In an attempt to achieve this assurance for the objectives and goals of an organisation, there are various types of controls that are employed by management on a day-to-day basis.

### 5.4.2 Types of Internal Controls

To assist in the achieving of the five objectives of the internal control system, detailed previously, four types of internal controls are generally employed, namely; preventative, detective, corrective and monitoring (Medical College of Wisconsin, 2001, online).
Preventative internal controls are there to avoid errors and irregularities in the operations of the organisation. Detective internal controls are used to identify those errors that have already occurred. Corrective internal controls are then used to correct those deviations that have previously been identified. The final type of internal control used is the monitoring control, which alerts management that a condition has occurred that is outside the prearranged set of restrictions (Medical College of Wisconsin, 2001, online).

These four types of internal controls, which form part of the overall internal control system, can assist management in the achievement of the goals of its organisation. Furthermore, senior management has certain responsibilities with regard to the internal control system it implements in the organisation.

5.4.3 Management’s Responsibility for an Internal Control System
After an internal control system is put into place in the organisation, its effectiveness needs to be monitored to guarantee that these controls continue to be satisfactory and function properly (RITS, 2000, online). It is ultimately senior management who is responsible for ensuring that internal controls are established and working to achieve the vision and objectives of the organisation (University of Rochester, 1996, online). The attitude and behaviour of senior management towards internal controls is crucial to the success of an internal control system.

An internal control system is more likely to succeed if management believes that those internal controls are necessary and important to the organisation. Senior management must communicate its beliefs to all employees in the organisation. Therefore, if management believes that internal controls are unrelated to the achievement of goals, then this attitude will be directly or indirectly communicated to employees as well. Employees may then view internal controls, which are used for risk management, as obstacles (RITS, 2000, online). Therefore, to ensure that an internal control system is successful in an
organisation, senior management must communicate to the employees how important the system is to their organisation.

Risk management and an internal control system go hand in hand. Senior management has a duty towards the organisation to be responsible for risk management and to ensure that an effective internal control system is in place in the organisation. These internal controls attempt to protect all the assets of an organisation, one of which is information.

Increasingly, organisations have become very dependent on information. Together with an organisation’s increasing reliance on electronic information comes the concern for the security of that information (Robiette, 2001, online). The protection of this information should be done, primarily, through the process of risk management and the internal control system that is associated with this. From the above discussion, it can be concluded that senior management should manage the organisation using effective corporate governance practices, one of which is risk management complemented by an internal control system. The main purpose of risk management and an internal control system is the controlling or reducing of risks associated with the assets of an organisation. Information is a key asset and is often described as the lifeblood of organisations. Therefore, it can be concluded that, by using good corporate governance practices, senior management is responsible for protecting information by means of risk management and an internal control system.

It was also highlighted in this section that for an internal control system to be effective, the necessary policies, methods and procedures must be in place to ensure the achievement of the main objectives of the internal control system. The following section will investigate the policy required to ensure the protection of one of the most important assets to an organisation – information.

### 5.5 Corporate Information Security Policy

As stated in Chapter 3, according to good corporate governance practices, senior management is responsible for providing direction and guiding an organisation in the
achievement of its objectives and goals. This guidance is usually accomplished through
the creation and implementation of management policies. One such policy is the
Information Security Policy. A Corporate Information Security Policy is one of the most
basic components of information security, since a suitable Information Security Policy
and the resulting procedures are central to the creation and establishment of an effective
information security program. The practices and procedures outlined in the Information
Security Policy should reflect the general policies of the organisation, as the entire
organisation should be striving to achieve the same goals (Krause & Tipton, 1998,
online). The Information Security Policy is a direction-giving document and should
define the objectives and boundaries of the information security program. Additionally,
itis should indicate management’s commitment and support for information security and
should describe the role that the policy plays in reaching the organisation’s vision (Höne,
2003, CD-ROM; BS 7799-1, 1999, p 5).

The Information Security Policy should define confidential information and clearly
define the role that management and employees should play in protecting the information
(Gordon and Glickson, 2001, online). The following subsection highlights how
important a Corporate Information Security Policy is to an organisation.

5.5.1 Importance of the Corporate Information Security Policy
An effective Corporate Information Security Policy should describe a framework
to direct the use and protection of an organisation’s information assets. This
direction-giving document should provide guidelines on how to manage
information security risk at a level acceptable to the organisation. Proactively
addressing information security issues in the digital era is not just good business
practice, it is a necessity for any organisation (Gordon and Glickson, 2001,
online).

A Corporate Information Security Policy is a high-level document that ultimately
leads to the enforcing of information security in a predefined and organised
manner. This is achieved through additional policies, such as an access-control policy (Zylt, 2001, online).

An additional motivation for a Corporate Information Security Policy is that it provides a structure within which various roles and responsibilities, in terms of information security, can be defined. A Corporate Information Security Policy should also make the organisation’s attitude to any actions that threaten the security of information assets explicit (Robiette, 2001, online).

An Information Security Policy could also be important for those organisations that are required to adhere to certain legal issues, where failure to have an Information Security Policy is illegal and leads to harsh consequences (Zylt, 2001, online). As seen in Chapter 3, one of the main tasks of senior management is to ensure that the organisation is adhering to any laws or regulations that apply to the organisation. Therefore, senior management must be responsible for the establishment of a Corporate Information Security Policy in the organisation.

As stated in this section, a Corporate Information Security Policy is a direction-giving document which outlines the procedures required for information security. Moreover, as outlined in Chapter 3, direction-giving is a function of senior management. Therefore, this Corporate Information Security Policy should assist senior management in guiding the organisation in the achievement of information security objectives. In guiding an organisation in achieving its objectives, senior management must, at the same time, ensure that the organisation is adhering to any laws or regulations that apply to it. The following section will explore legal accountability in terms of information security.

5.6 Legal Accountability for Information Security

As already discussed, one of the main functions of senior management is to define the vision for the organisation and direct the organisation in the achievement of this vision. As seen in the previous section, the Corporate Information Security Policy is a direction-giving document with regard to information security. Therefore, an Information Security
Policy, if implemented properly, assists senior management in achieving the vision set for information security.

Therefore, creating and implementing an Information Security Policy is incredibly important for any organisation. In addition, in some circumstances, a court of law may find that an organisation without an Information Security Policy or practices in place has failed to take the necessary steps to protect its trade secrets (Gordon and Glickson, 2001, online).

Therefore, to reduce liability an organisation should develop and maintain a comprehensive Information Security Policy that sets the direction for the protection of information. This should help protect an organisation from prosecution as the overall cost of developing an Information Security Policy is generally lower than the cost of responding to a single summons and complaint in litigations if a security breach were to occur (Gordon and Glickson, 2001, online). However, the question is: who is legally accountable for information in an organisation?

As concluded previously, the senior management of an organisation is accountable and/or responsible for the protection of the information assets of an organisation. Furthermore, organisations that do not show due diligence in reducing their exposure to risks associated with information will almost certainly become targets for lawsuits when security breaches have occurred. If an organisation were to be taken to court it is senior management who is legally accountable for information and who will have to give an account in court regarding the protection of the information. In a case where an organisation has become the target of a lawsuit involving breaches in information, senior management must be able to prove that it has set the necessary direction for information security in the organisation. Secondly, senior management must have ensured that the relevant resources were made available to assist in the protection of information. It is also vital for senior management to ensure the Information Security Policy and practices of the organisation comply with international guidelines and codes of practice - for
example, ISO/IEC 17799 (Zylt, 2001, online). By doing so, senior management will help reduce the liability of the organisation.

As highlighted in Chapter 2, criminal prosecution of the perpetrator who caused an information security breach will not compensate an organisation for the losses resulting from the breach. This breach in confidential information, for example, could also result in damage to an organisation’s reputation. Therefore, protecting information, through an effective Corporate Information Security Policy, actually results in the protection of the organisation itself. As seen in Chapter 3, senior management is responsible for the protection of the organisation and the assets belonging to the organisation. Therefore, senior management, as part of its corporate governance duties, should ensure that an effective Corporate Information Security Policy is in place in the organisation. In doing so, senior management can ensure that the organisation is not exposed when it comes to the legal implications of information security.

5.7 Conclusion

As highlighted in Chapter 3, one of the duties of senior management is to protect the important assets of the organisation. Furthermore, as detailed in this chapter, senior management accomplishes the protection of the assets in the organisation through a process of risk management and an internal control system. Risk management identifies the risks facing the assets of an organisation and determines how best to minimise or eradicate them. The mechanism for controlling and reducing the risks, identified during the risk management process, is an internal control system. As highlighted in Chapter 2, the information possessed by an organisation is among its most valuable assets and is critical to its success. Therefore, senior management, who is responsible for the organisation’s success, is ultimately responsible for the protection of its information.

Unless senior management has done everything possible and made the necessary resources available to facilitate an adequate level of information security, it cannot delegate its information security duties. The protection of information, primarily, can be achieved through the creation of a Corporate Information Security Policy and this
commitment from senior management to information security should result in the formally agreed upon Information Security Policy. This Corporate Information Security Policy outlines the goals for the information security program, as well as the responsibilities of all people involved in the organisation.

As detailed in this chapter, protecting the information of an organisation would contribute towards the protection of the organisation itself. It is the duty of senior management, through effective corporate governance practices, to protect the organisation and all its assets, one of which is information. Thus, it can be concluded from this chapter that to adequately protect its organisation, senior management must be responsible for the protection of information through effective information security practices.

The following chapter will investigate the fields of corporate governance and corporate culture, the effect that management policies and the example set by senior management has on the corporate culture, as well as the importance of assessing the current corporate culture in the organisation. The following chapter will conclude with an overview of how a corporate culture can be transformed by senior management.
6.1 Introduction

Chapter 3 explored the field of corporate governance. Chapter 4 explored the field of corporate culture. Both these previous chapters investigated these fields individually. The chapter on corporate governance explored the importance of corporate governance and the threats to the field. The four pillars that are required for the effective governance of an organisation, namely accountability, responsibility, fairness and transparency, were also discussed. It was established in Chapter 3 that one of the main aims of corporate governance is to endorse the efficient use of assets and to ensure accountability for the management of those assets. It was also concluded that good corporate governance practices are essential in cultivating a sturdy corporate environment. The corporate culture chapter explored various definitions of
culture and the three levels of culture. The different types of culture, the functions of culture and the importance of corporate culture were discussed in the chapter. The chapter established that the corporate culture directly influences the actions and behaviour of the employees in the organisation. However, it is no longer sufficient to discuss these fields individually. They must be investigated in relation to one another.

As seen in Chapter 4, the values expressed at the Espoused Value level of culture are the values and principles the organisation would like to promote. As these values reflect the vision of the organisation, and policies should also reflect the vision of the organisation, it follows that the espoused values of an organisation should be expressed in the policies of an organisation. However, as was also seen, those values that an organisation hopes to endorse may be different from the beliefs and norms expressed in the actual behaviour of the employees. Therefore, the organisation’s culture is not necessarily the set of espoused values of the organisation (Hagberg Consulting Group, 2002, online). As a result, not unlike other assets in an organisation, human resources (the employees) have to be managed strategically. The resulting benefits of this approach can be high retention rates and strong corporate value systems (Schafer, 2003, online). As a result of the need for employees to be managed strategically, the corporate culture, which influences the behaviour of these employees, must be supervised by senior management.

This chapter will investigate the role that senior management plays in influencing the culture in the organisation and the relevance of the correlation between corporate governance and corporate culture. It will investigate the general policies created by management and how these policies affect the corporate culture and, therefore, also employee behaviour. The challenges and the ability and need for management to transform culture will also be investigated.

6.2 Shaping Corporate Culture

There are many factors in an organisation that help in the shaping of the culture of an organisation. One of these factors is senior management. As seen in Chapter 3, Corporate Governance, senior management is accountable and responsible for the
management of all aspects of the environment in which it operates. And as seen in Chapter 4, Corporate Culture, this working environment of an organisation is, to a large extent, determined by the corporate culture. The following section will examine the factors that shape the corporate culture of an organisation and how corporate governance plays a part.

Senior management, using effective corporate governance, has a crucial role to play in shaping the culture of the organisation, whether management realises it or not, and it is vitally important for senior management to fully understand the corporate culture of the organisation. Understanding the corporate culture could prove to be the difference between the failure and success of an organisation (Hagberg Consulting Group, 2002, online).

Corporate culture – the attitude to finance, employee welfare and technological change - effects organisations in two crucial ways. The first is through legislation and, second, through its own decision making. The effects of legislation on an organisation are direct and can be identified. As seen in Chapter 4, culture defines what behaviour is acceptable and what is not acceptable. Therefore, legislation represents the culture of a country, by defining what can and what cannot be done. Consequently, an organisation must adhere to the legislation that affects it; otherwise legal action could be taken against it. Not adhering to this legislation would have a direct and visible consequence for the organisation. However, the effects of culture on an organisation’s decision making are indirect and invisible and can be difficult to assess. Matters of culture are elusive and difficult to pin down, but no less important than legislation issues (Policy Studies Institute, 1999, online). Chapter 3 highlighted that senior management must ensure adherence to the relevant laws that apply to the organisation and is accountable and responsible for decision making and strategic planning. As culture effects the organisation in terms of legislation and decision making, it is necessary for senior management to understand the role that it plays in shaping the corporate culture.
As seen in Chapter 4, only five percent of organisations have a definable culture, where senior management plays an active role in actually shaping the culture. This could be as a result of the fact that senior management does not realise the impact and effect that it has on the corporate culture. It is extremely important for senior management to realise that the culture of an organisation is not formed by what it, as senior management, preaches or publishes in policies, but what it accepts in practice (Drennan, 1992, p 3). Often, the strongest indicators of a corporate culture are the issues that senior management pays attention to or avoids. For example, if the CEO of an organisation tends to avoid conflict – the same behaviour will permeate the organisation. The behaviour that senior management displays will strongly shape the culture and practices of an organisation (Hagberg Consulting Group, 2002, online).

The behaviour of senior management is often different to the values expressed in management policies. This would be an instance where senior management does not follow the rules set out in management policies. As a result, employees would observe the behaviour of management to determine how they should behave, consequently, ignoring management policies (Hagberg Consulting Group, 2002, online). Therefore, the behaviour of employees in an organisation depends, primarily, on the behaviour displayed by senior management, more than the principles and practices set out by senior management in policies. Senior management ignores at its peril the effects of its behaviour on employees (Brooks, 1997, online). The behaviour demonstrated by senior management, although a large contributor to the culture, is not the only influencing factor on corporate culture. The behaviour of fellow employees also influences the corporate culture to a certain extent.

Indications of an ideal culture would be one where the actions and behaviour of the employees match the guidelines detailed in the organisation’s policies. As highlighted in Chapter 4, this would mean that the Shared Tacit Assumptions level of culture is in line with the Espoused Value level of culture, where the behaviour of the employees is in line with the policies set out by management. If the actions of employees do not match the set policies, a new employee joining the organisation will soon match the behaviour of their
peers and they will not pay attention to the policies (Drennan, 1992, p 18). When there is a discrepancy between the policy and the behaviour of fellow employees, an employee can deduce that employee behaviour is the behaviour that is accepted by management. Therefore, the behaviour that management accepts in practice, as well as the behaviour management demonstrates, to a large extent, becomes the corporate culture.

The following section will discuss the policies where management specifies the values that will be espoused by its organisation and the role that these policies play in corporate culture.

### 6.3 Management Policies and Corporate Culture

One of the main functions of senior management in terms of good corporate governance is to guarantee that policies and procedures are in place in the organisation to protect its assets. It is also the responsibility of senior management to establish a clear purpose and vision for the organisation. As seen in the previous section, the behaviour that senior management accepts in the organisation contributes greatly to the shaping of the corporate culture. This is because the desire to conform to management expectations is a powerful driver of employee behaviour and, therefore, a powerful driver of corporate culture (Drennan, 1992, p 23).

The purpose and vision of an organisation, together with management expectations, should reflect the content detailed in all the management policies for the organisation, so that employees would want to shape their behaviour according to the content of management policies. Organisational procedures and policies, therefore, are necessary as guidelines for employees to understand the role they should play in their organisation and to help employees do a consistently good job (Drennan, 1992, p 23).

It is extremely important for the behaviour of the employees and the content of the management policies to correlate. These policies must be carefully planned and implemented in the organisation as the first step to being effective. The next step is to ensure that the policies are enforced. As detailed in Chapter 3, one of the main functions
of senior management is to guide the organisation in achieving its goals. The management policies created and approved by management must be enforced by senior management to assist the organisation in achieving its goals. Therefore, it is management’s attitude towards policies that influences the corporate culture in the organisation. If management treats policies as window-dressing, or if they see policies as a waste of time, then the employees will obviously treat the policy with the same disregard. Conversely, if management describes exactly what is expected from the employees and continually expresses how important the policies are, then employees will follow suit and a culture similar to what is detailed in policies should develop (Drennan, 1992, p 17). This would result in the alignment of the behaviour of the employees and management expectations for the achieving of organisational goals.

The way the policies are implemented in an organisation will also affect the corporate culture. If a culture is positive and constructive it can motivate employees to do their jobs to the best of their abilities, and in the process help to achieve the organisation’s goals. However, if policies are implemented rigidly they deprive employees of the authority to act quickly in difficult situations. This could create a culture that is very restrictive to the employees which could lead to dissatisfaction, resulting in employees being less inclined to work towards the organisation’s goals (Information Technology and Management, 1999, online). Restrictive policies may also imply a lack of confidence in the employees’ ability to do a good job. Therefore, although the procedures and policies of an organisation have a prime role in shaping its corporate culture, they can also be a main source of employee frustration. Management needs to find the balance in its organisation, both in the creation and implementation of the management policies and in the enforcement of the policies, to create an environment in which employees will find satisfaction in their management policies (Drennan, 1992, p 23).

As seen in this section, the desire to conform to management expectations is a powerful driver of employee behaviour, consequently resulting in a powerful driver of the corporate culture. These management expectations should be outlined in the policies of the organisation, which means that the behaviour of employees should conform to what is
written in the management policies. Therefore, management policies should influence the shaping of the corporate culture of an organisation.

The question is: how will senior management know if employees are satisfied with management policies and are adhering to them? As detailed previously, it is vital for management to understand the corporate culture in the organisation. A key to this understanding is an assessment of the current culture in the organisation. The following section details the importance and types of cultural assessment that can be performed.

### 6.4 Cultural Assessment

It is critically important for the corporate culture of an organisation to be understood by senior management. If an organisation wants to capitalise on its ability to achieve its objectives, it must know if the existing culture supports and drives the actions and behaviour necessary to achieve its strategic goals. Cultural assessment can enable an organisation to analyse the gap between the current culture in the organisation and the desired culture perfect for achieving its objectives. Developing a picture of the ideal and then taking a rational look at the gaps is vital information that can be used to design practices to close the gaps and bring specific elements of culture into line (Hagberg Consulting Group, 2002, online). As seen in previous chapters, the vision of an organisation represents an idyllic future for the organisation. Senior management is responsible for defining and achieving this vision. Therefore, it is tremendously important for senior management to perform a cultural assessment to identify how actions and behaviour need to change to achieve this vision.

When the senior management of an organisation wishes to perform a cultural assessment, there are two approaches that could be used to gather information about the current culture.

- The first approach is the *anthropological* approach. With this approach, the methods used to assess an organisation’s culture entail that the person or group performing the assessment should immerse themselves in the corporate culture
they are assessing. They study the first level of corporate culture, the cultural artifacts, and gather information on the culture according to what they observe in the organisation. This approach must be performed by someone outside of the organisation. This is because management and employees are so absorbed in their corporate culture that they lack the perspective and ability to provide reliable information on their culture (Beach, 1993, p 35).

The second approach is the psychological approach to cultural assessment. This approach focuses not on the artifacts of the culture, but rather on what employees think of the culture. This assessment uses simple tests or questionnaires. The psychological approach determines the ‘personality’ of an organisation, which is its culture (Beach, 1993, pp. 36-37).

Both approaches have their disadvantages. The anthropological approach is very time consuming as the persons performing the assessment, called the anthropologists, must ‘live’ the corporate culture to understand it. Another drawback is that the anthropologist might have pre-existing cultural assumptions when assessing the organisation’s culture and may assess the culture in a biased fashion (Beach, 1993, p 35).

A disadvantage of the psychological approach is that it involves defining a ‘personality’ for the organisation. Defining a ‘personality’ could be controversial, because even when defining a personality for an individual it is based on the person doing the assessment. Therefore, different observers could observe the same behavioural characteristics and draw different conclusions (Beach, 1993, pp. 36-37).

Regardless of which approach is used, cultural assessment can provide measurable data about the real organisational values and norms of which senior management should be aware. Senior management may have illusions about the culture in the organisation and, by examining the cultural assessment, management may find that it is not practicing what it preaches (Hagberg Consulting Group, 2002, online). If this is the case, then
management may need to transform the corporate culture into one that is in line with its management policies.

6.5 Transforming Culture

If a cultural assessment has been performed in an organisation and the results identify a large gap between the actual culture and the ideal culture, management may need to attempt a change in the behaviour and attitudes of employees, and, therefore, attempt to transform the culture in the organisation. Important to note, is that there is no right or wrong culture, except in relation to the environment in which the organisation operates (Schein, 1999, p 21). Therefore, what works for one organisation may not work for another. The transforming of corporate culture into one that will operate best in its chosen environment will be investigated in this section.

Employee behaviour and attitudes are largely a result of the internal environment in which they work. External factors, however, also have an influence on the employee mind-sets. For example, if unemployment in the external environment increases, the employees’ behaviour may temporarily become agreeable and accommodating. However, it is still the internal environment in the organisation that has the most influence on employees’ attitudes. That is why the power to change corporate culture lies principally in the hands of senior management (Drennan, 1992, pp. 3-4).

As detailed in Chapter 4, as an organisation grows, the relationship between its activities and its culture becomes more complex and a sense of direction begins to develop. This sense of direction or the agenda that senior management of an organisation wants to pursue is termed its vision. Activities, culture and vision become an interrelated whole, each interacting with and shaping the other. Culture embodies the organisation’s fundamental beliefs and the activities and behaviour that result from these beliefs (Beach, 1993, p 50). Therefore, the culture influences the activities of the organisation and, equally, the manner in which the activities are carried out influence the culture. As an organisation matures and develops its own unique culture, a distinction can be made between the different types of activities in the organisation.
The first type of activity is tactical activities. These activities focus on immediate goals, where the result of the activity will be tangible. For example, hiring someone to fill an open position in the organisation.

The second type of activity is operational activities. These activities are directed at longer-term goals. For example, changing the way a particular procedure is executed to improve performance.

The third type of activity is strategic activities. These activities focus on long term goals that could shape the future of an organisation. For example, implementing a new process or procedure to enhance the organisation.

In order to change the corporate culture of an organisation, the activities of the organisation must be understood. This is to ensure that the activities that require changing in the organisation can be properly identified (Beach, 1993, p 17). Once the activities and culture of an organisation are well defined, the vision that management has for the organisation requires attention.

Vision defines the ideal future. This vision might imply that the current culture be kept the way it is or it might imply the need for change in the organisation. This means that the vision might need nothing more than the natural evolution of the present culture, or it may require drastic changes in what the organisation is doing – and perhaps, therefore, in the organisation’s culture (Beach, 1993, p 17).

The task of transforming the culture takes vision, commitment and determination. Without this combination it will not happen, and it certainly will not last (Drennan, 1992, p 4). If an element of corporate culture needs to be changed, it is important that senior management realise it is tackling one of the most stable areas of an organisation. The corporate culture is so stable because it represents the accumulated learning of a group. Chapter 4 investigated the three levels of culture and this accumulated learning of a group
is found at the Shared Tacit Assumptions Level of culture and includes all beliefs, principles and values that the employees share. Many of the most important aspects of culture are essentially invisible which makes transforming culture very difficult (Schein, 1999, pp. 21-26).

Changing and transforming corporate culture is a massive task. Employees prefer structure in the work environment, to have a known framework within which to work so that they can adapt their behaviour to deal with their environment successfully. Even when the environment has its unpleasant features, employees find comfort in the fact that they know the environment and what to expect. Apprehension arises when there is the prospect of a big change in the environment that employees know so well (Drennan, 1992, p 9). Any prospective change in an environment in which employees are comfortable could lead to massive amounts of anxiety and resistance to change. For an organisation’s corporate culture to change, it involves the unlearning of beliefs, values and assumptions and a change in attitude (Schein, 1999, p 26). Employees prefer stability in their environment and the traditions that are inherent in this environment are difficult to change. These traditions play a large part in shaping the corporate culture of an organisation (Drennan, 1992, p 9).

Employees of an organisation may be coerced into changing their obvious behaviour, but this behavioural change will not become established until the deepest level of culture, the Shared Tacit Assumptions level, experiences a transformation (Schein, 1999, p 26). This is where senior management, using effective corporate governance practices, should exercise its influence.

Senior management must ensure that the policies of the organisation are in line with the vision for the organisation. Senior management should then enforce these policies so that they become part of the way things are done in the organisation. As seen in Chapter 3, the pillars of accountability and responsibility are essential components of good corporate governance. These pillars should be used by senior management to help enforce its policies, so that employees know that they will be held accountable and/or responsible for
their actions regarding management policies. However, it is not enough for senior management to only enforce its policies - it is important for the attitudes of senior management to encourage this change in the corporate culture. If nothing changes in the procedures of the organisation or the attitudes of its management, employee attitudes will not change either (Drennan, 1992, p 3). There are, however, a few facts which must also be taken into consideration.

Even if the procedures and attitudes of senior management change, when endeavoring to revolutionise the corporate culture in the organisation, senior management should ensure that employees understand the benefits of changing the way things are done in the organisation. Employees resist change because it is an uncomfortable and anxiety-producing process (Schein, 1999, p 26).

A new corporate culture cannot simply be ‘created’. Senior management can demand or encourage a new way of working and thinking, management can monitor the changes to make sure that they are done, but employees of the organisation will not internalise the changes and make it part of the new culture unless they understand the benefit of these changes. It is senior management’s responsibility to highlight that the changes needed in the current culture are worthwhile and important (Schein, 1999, p 187).

6.6 Conclusion

As highlighted in Chapter 4, culture exists in an organisation at both conscious and unconscious levels and many organisations have a culture that exists by default. This default culture can change by accident and is usually influenced by a few key people in the organisation. This is neither beneficial nor productive for an organisation.

It can be concluded from this chapter that, whether senior management is aware of it or not, management greatly influences the corporate culture in the organisation and should make a concerted effort to transform the corporate culture into one that will help in the achievement of the organisation’s goals.
As part of good corporate governance practices, one of the responsibilities of senior management is that it must outline the goals and vision for the organisation. However, its responsibility should not end there. Senior management must also guide the organisation in the achieving of these goals. The activities and behaviour of the organisation’s employees play a large part in obtaining the organisation’s goals. Therefore, senior management, as part of its corporate governance duties, should ensure that the necessary elements of corporate culture are in place to support the organisation in achieving its goals.

As seen from this chapter, the policies of an organisation should outline these goals and vision for the organisation. A mutual relationship exists between the activities and culture of an organisation. Therefore, it can be concluded that if senior management can transform the activities of its employees, their behaviour will change and it will ultimately transform the culture. Most often, employees will model their behaviour on the behaviour demonstrated and accepted by senior management. Therefore, senior management must also ensure that its behaviour reflects the policies in the organisation.

Very important to note from this chapter as well, is that the power to change and transform the culture in an organisation is held by senior management. However, corporate culture is probably one of the most stable parts of an organisation and, therefore, one of the most difficult to change. It is difficult to change, because it represents the beliefs and values accepted by everyone in an organisation and changing of these beliefs will not happen overnight. A cultural assessment should be conducted in an organisation to identify the difference between the current culture and the ideal culture. Senior management, using good corporate governance practices, can then use this difference to attempt to transform the corporate culture into one that will help the organisation attain its goals.

The following chapter will investigate the fields of information security and corporate culture. The need for the integration of the two fields and the current attitude and behaviour of employees towards information security will also be investigated. The
effect that the Information Security Policy has and should have on the corporate culture will also be explored and the chapter will conclude with an investigation of information security awareness.
Chapter 7: Information Security and Corporate Culture

7.1 Introduction

As highlighted in Chapter 4, culture within an organisation exists at three levels. The Artifacts level of culture demonstrates the visible behaviour of employees. This behaviour is directly influenced by the beliefs and values of the employees found at the Shared Tacit Assumptions level of culture. Therefore, the corporate culture of an organisation, shaped by the beliefs and values of employees, directly influences the behaviour of employees. The chapter on information security, Chapter 2, explored the importance of information security and the risks to the important asset of information. This chapter also highlighted that in order for information security to be effective; it takes a whole-hearted effort from the entire organisation – senior management and the rest of the employees included.
Information security has increased in importance in recent years, and, in the past, physical and technical controls may have been sufficient to protect the electronic information of an organisation, but today these are no longer enough. To adequately protect information assets operational controls are required. Operational controls determine the actions employees must use in order to sufficiently protect information. The effectiveness of information security controls depends on the competency and dependability of the people who are implementing and using them. Therefore, to a large extent, the behaviour and actions of employees determine the effectiveness of information security practices (Dhillon, 2001, p 165). Senior management of organisations, in particular, has tended to view information security as a technical problem confined to the Information Technology department.

However, to be effective information security needs to become part of the way everyone conducts their daily business, from management at the top, right throughout the entire organisation. The act of protecting information should become second-nature to the management and employees of an organisation. This is because the information that resides on an organisation’s systems is owned by the organisation as a whole, not just the IT department, and should therefore be valued and protected by everyone (Deloitte & Touche, 2002, online).

The chapter will investigate the need for the incorporation of information security into corporate culture and the effect employee behaviour has on the organisation will also be investigated. The effects of the Corporate Information Security Policy on corporate culture will also be detailed and the chapter will conclude with an investigation into the importance of an information security awareness program. This awareness program should result in behavioural changes of employees which should be in line with the Corporate Information Security Policy.
7.2 The Need for the Integration of Information Security and Corporate Culture

Physical and technical controls are tangible controls that attempt to enforce compliance with information security practices and procedures in an organisation, but it is really operational controls and the resulting behaviour and actions of the employees and the processes they use that can sustain information security practices (Deloitte & Touche, 2002, online). Therefore, it is the behaviour and actions of employees that makes information security successful or not. As seen in Chapter 4, the behaviour of employees is shaped, to a large extent, by the beliefs and values found at the Shared Tacit Assumptions level of corporate culture. Therefore, if the Shared Tacit Assumptions level of corporate culture can be changed, the behaviour of employees would change at the Artifacts level.

Working in an organisation is essentially working in a team, where all employees should be working towards the achievement of the goals and objectives of the organisation. Further, just as in any team situation, the team is only as strong as its weakest link. As pointed out in Chapter 2, one hundred percent compliance to information security practices will never be a reality. This is largely due to the fact that, often, the behaviour and actions of employees and the information security processes they use in their daily work represents the weakest link in the information security process (Martins and Elof, 20 October 2002, Information Security Culture, e-mail). Information is a valuable asset and even the most sophisticated computer security systems are vulnerable to human interference (Deloitte & Touche, 2002, online). Therefore, in an attempt to minimise the impact that inappropriate actions and behaviour has on an organisation, it is extremely important for information security practices to become an interrelated component of the corporate culture that exists in organisations.

As highlighted in Chapter 4, corporate culture controls employees more than the employees control the culture. Corporate culture, to a large extent, determines what behaviour is acceptable in an organisation. Once employees learn and understand what behaviour is accepted in their organisation, they develop beliefs and assumptions that
slowly phase out of their conscious thinking and become tacit rules as to how their jobs should be done. These beliefs and assumptions are found at the Shared Tacit Assumptions level of culture. Therefore, for the corporate culture to evolve and protect the information assets of an organisation, the accepted behaviour and actions of employees must also evolve. The behaviour that is acceptable in an organisation should be reflected at the Espoused Values level of the corporate culture. The employees will subsequently develop beliefs and assumptions regarding the new information security practices, which should become second-nature behaviour to them by becoming part of their Shared Tacit Assumptions level. Therefore, the Espoused Values level of culture should correspond with the Shared Tacit Assumptions level of culture. The effect that this employee behaviour, observed at the Artifacts level of culture and influenced by the Shared Tacit Assumptions level, has on information security will be investigated in the following section.

7.3 Employee Behaviour and Information Security

As seen in the previous section, employee behaviour and actions can often be the weakest link in the information security chain. Human threat to information can be both accidental and malicious. Many of these threats originate outside an organisation and can be addressed through physical and technical controls, as well as through the Corporate Information Security Policy. This is because an Information Security Policy should help the employees understand their responsibilities and should guide them to adopt the correct behaviour that will ensure the protection of the valuable asset of information (Symantec Corporation, 2001, brochure). The Information Security Policy and its effect on corporate culture will be detailed in a later section.

Even though many of the threats to information originate from outside an organisation, the threats posed and the damage done by employees inside an organisation is more common. One of the main reasons for this is that legitimate employees have greater access to information (Symantec Corporation, 2001, brochure). As seen in Chapter 5, greater access to information exposes organisations to new threats and risks regarding the protection of their information. Organisations depend on information to carry out their
daily activities and this critical information is now in the hands of a much larger number of employees, and it is stored in remote and dispersed locations (Deloitte & Touche, 2002, online). Employees who now perform tasks that were previously handled by highly trained specialists have generally received little or no training in the most common information security practices. Therefore, it is vitally important that employees understand and are aware of the importance of the information in their organisation. In addition, employees must understand how their behaviour and actions influence the success of information security practices in their organisation.

One of the ways to combat the human threat to information is through an Information Security Policy. The following section will investigate the effect the Corporate Information Security Policy has, or should have, on corporate culture.

7.4 Effects of Corporate Information Security Policy on Corporate Culture

The Information Security Policy must outline the vision senior management has for the organisation in terms of information security. Therefore, the Information Security Policy should influence the Espoused Values Level of culture in terms of information security, as it is at this level that the vision and goals are expressed. The Corporate Information Security Policy must work within the organisation where this culture exists. Therefore, there is no generic Information Security Policy that can be applied to all organisations, as each corporate culture is unique. The Information Security Policy must address the security needs of the specific organisation (Deloitte & Touche, 2002, online).

Once the policy is created, the understanding of the corporate culture around information security becomes essential for the successful implementation of information security practices in an organisation. Assessing the employees’ awareness, capability and commitment to information security will determine the best means for the delivery of the Information Security Policy so that it will be effective in the organisation (Deloitte & Touche, 2002, online). Therefore, assessing the corporate culture in terms of information
security will determine the best means for introducing information security practices in an organisation.

To have an effect on the corporate culture of an organisation, the Information Security Policy must define what behaviour is and is not allowed, by whom and in what circumstances in terms of information security. Users of information systems, the employees, would be more willing to adhere to better security practices, if they were more knowledgeable about what good information security practices actually involved (Robiette, 2001, online). Therefore, the Corporate Information Security Policy should detail the importance of protecting information and the information security practices necessary to accomplish this. This would attempt to ensure that business plans and other confidential information is protected from theft or unauthorised disclosure. The details of the Corporate Information Security Policy would allow employees to become more knowledgeable about security practices and encourage them to adhere to these practices.

If the employees adhere to good information security practices, their behaviour will be beneficial to the protection of information. Thus, an Information Security Policy should have a major influence in cultivating the appropriate corporate culture for an organisation, and should have at least two main objectives. Firstly, as seen previously, an Information Security Policy should educate employees, particularly non-technical employees, about the risks to information inherent in their daily jobs. Often, loss of confidential information can be avoided when employees are alerted to the subtle, but often devastating, threats before them. Secondly, an Information Security Policy should establish the organisation’s official perspective regarding the protection of information, and give the organisation grounds for disciplinary action or legal defences should the policy be violated (Gordon and Glickson LLC, 1997, online).

As seen previously, an Information Security Policy should reflect the vision, or the corporate philosophy for an organisation’s critical information (Symantec Corporation, 2001, brochure). Furthermore, although no organisation can guard against all the possible risks related to protecting information, a carefully constructed Information
Security Policy can establish the foundation of a corporate culture that is able to lessen many of the threats to information (Gordon and Glickson LLC, 1997, online). The Information Security Policy assists in the creation of an information security conscious corporate culture by specifying what behaviour is acceptable and what behaviour is unacceptable in terms of information security.

The behaviour of employees towards information security is influenced by their beliefs and values regarding information, which is found at the Shared Tacit Assumptions level of culture. As seen previously, the vision for information security is found at the Espoused Values level of culture. Therefore, to achieve the vision for information security, the Espoused Values Level and the Shared Tacit Assumptions level of culture should be aligned, so that the employees’ behaviour at the Artifacts level will support the vision for information security. To do this, a comprehensive Information Security Policy, one that is written in conjunction with an organisation’s other management policies and implemented and enforced properly must cultivate the corporate culture that is necessary in limiting the exposure of information to risk (Gordon and Glickson LLC, 1997, online).

However, an Information Security Policy which is too restrictive is unlikely to be successful, since many employees find it difficult to work under such conditions. Nevertheless, an Information Security Policy which is too slack will leave the organisation open to abuse. A successful Information Security Policy will generate a high degree of consensus amongst all of those involved, and should foster a positive attitude towards information security in terms of its benefits to the organisation (Robiette, 2001, online).

Once a Corporate Information Security Policy has been created, compliance with that policy must be ensured. Employees must be made aware of the policy and the importance of the policy should be stressed to the employees. Without this awareness and education of employees, the corporate culture will not change (Deloitte & Touche, 2002, online). Therefore, information security awareness is extremely significant and the
following section details the major characteristics and importance of information security awareness.

It is pertinent to investigate information security awareness in the following section as employees who are not aware of the importance of information will not adequately protect information assets. However, an information security awareness program should not be used to simply make employees aware, but as a mechanism to shape the behaviour of employees towards information security.

7.5 Information Security Awareness

There are a number of controls that can be implemented in organisations to protect information from unauthorised individuals. However, as seen previously, it is the authorised employees who may pose the biggest threat. These authorised employees have the necessary privileges to access the information and are often careless with these privileges, which leads to the information being at risk. Having an ongoing information security awareness program in place can greatly reduce these risks. However, as seen previously, many of these risks cannot be addressed through physical or technical controls – it is the operational controls and consequently the human element that must be addressed (Security Awareness Incorporated, 2003, online).

To attempt to address this human element, senior management must communicate the Information Security Policy to all employees to heighten their awareness. When employees fail to do what management expects in terms of information security, it is very often the result of ineffective communication, rather than the result of malicious intent on the part of the employees. To ensure the security of an organisation's information, learning opportunities must be provided in fundamental security concepts and practices. In addition to this, current and emerging security practices and the theory that acts as a foundation for them must be learned. Senior management and employees must be well versed in information security (Spafford, 2002, online).
In order to do this, an information security awareness program is possibly one of the most important weapons in communicating information security to the employees of an organisation. As seen previously, an organisation can have many physical and technical controls in place, but these will be worthless when employees are not even aware of the proper security procedures and practices (Security Awareness Incorporated, 2001, online).

It is not until each and every employee realises that what they do, how they do it and why they do it impacts the safety of the organisation’s assets that a security awareness program is successful. In order for an information security awareness program to be successful, the program should have certain characteristics. These characteristics will be discussed in the following subsections.

7.5.1 Educate and Inform Employees
The first characteristic is to educate and inform employees. From senior management down, the importance of information and information security needs to be conveyed. Information security policies, standards, guidelines, and procedures achieve their maximum effectiveness when steps are taken to ensure that all employees fully understand the reasons underlying their significance. Employees should also be directed as to where they can locate their organisation’s written policy, standards, guidelines and procedures (Security Awareness Incorporated, 2001, online). Therefore, for information security to be truly effective, the employees must be aware and understand the benefits of protecting the information in their organisation.

7.5.2 Achieve a Balance between Security and Productivity
The second characteristic is that a balance needs to be found between information security and productivity. As seen previously, when information security practices become too restrictive, they become burdensome and impede the productivity of the user community. Conversely, where security measures are nonexistent or too lax, information and information systems are vulnerable to
disruption, modification or destruction. Senior management needs to establish the level of risk it is willing to absorb, while also ensuring that the employees have the necessary access and authority to carry out the organisation’s objectives (Security Awareness Incorporated, 2001, online). Therefore, information security practices must protect the information of an organisation, while still allowing employees the freedom to do their jobs. In order to achieve this balance, employees must be made aware of the information security practices through the information security awareness program and it is vitally important for the employees to understand the information security program.

7.5.3 Communicate to Individuals the Importance and General Concepts of Security, without Inspiring Boredom
Information security awareness programs should include many realistic examples of security requirements and breaches. Otherwise, the employees might not fully pay attention to the details of the awareness program and the program will not be successful. The information security awareness program must appeal to the employees’ imagination, emotion, and sense of responsibility and logic. It must be remembered that the end goal of the information security awareness program is for employees to be left with a desire to be secure and a better understanding of how to do it (Security Awareness Incorporated, 2001, online). Therefore, it must become apparent from the information security awareness program that information security is everyone’s responsibility.

7.5.4 The Mindset of the Individual must be Addressed
Most employees are knowledgeable about physical security. However, as seen previously, it is not only physical controls needed for information security. It is extremely important, through the information security awareness program, that employees recognise the benefits of protecting the information in their organisation. Employees must realise that their behaviour and actions in protecting information affects not only themselves, but the organisation as a whole. One of the major reasons for the lack of information security awareness of
employees is the failure to understand what can be lost through security breaches (Security Awareness Incorporated, 2001, online). This is why it is so vitally important for good information security practices to become tacit rules for employees.

To be truly effective, an information security awareness program should address all the above characteristics (Security Awareness Incorporated, 2001, online). As seen from this section, an information security awareness program is very important in making employees of an organisation understand and become aware of the significance of their duties and behaviour regarding information security. As seen in Chapter 6, employees will only internalise changes to their environment and culture if they understand the benefits of these changes. Therefore, an information security awareness program should be used as a mechanism to shape the behaviour of employees. Thus, by making the employees understand and become aware of protecting the information in their organisation and the benefits thereof, it will assist in incorporating information security into the corporate culture of the organisation.

7.6 Conclusion

As seen in this chapter, employees, if not properly aware and informed about information security, can be the weakest link when it comes to sustaining information security practices. If employees do not understand the importance of protecting the information in their organisation, they may be careless in their information security practices and procedures. Also, although physical and technical controls are essential for effective information security, it is operational controls and the cultural and human aspects related to information security that really determine the sustainability of information security practices. It is, thus, vital for employees to understand the effect their actions and behaviour have on information security practices and, consequently, on the organisation as a whole.

The Corporate Information Security Policy should assist employees in understanding the role they play in information security by defining the roles and responsibilities that
should be undertaken to ensure the protection of information. Therefore, the Information Security Policy defines what behaviour is acceptable and unacceptable in terms of information security. The behaviour towards information that is acceptable should be compared to the current behaviour of employees, to highlight the changes that need to be made in the behaviour and actions of employees to adequately protect information.

However, it was also seen that employees will only internalise changes to the way they protect information if they understand and see the benefit of the changes. If employees internalise changes regarding information security practices, these changes will become second-nature to the employees and will accordingly become part of the corporate culture of an organisation.

It can, therefore, be concluded from this chapter that for information security to become an interrelated component of the corporate culture of an organisation, it is essential that employees are aware and have the desire to protect the information of their organisation. The employees in an organisation can be the weakest link when it comes to information security practices, but they can also be the best defense if handled correctly (Deloitte & Touche, 2002, online). Ultimately, therefore, successful information security practices should move out of the conscious thinking of employees and become implicit rules through which information is protected. Thus, information security becomes part of the overall corporate culture.

The following chapter will correlate the relationship between all three fields of corporate governance, information security and corporate culture. The relationships between the fields will be explored in detail and concluded. The chapter will conclude by defining the term ‘Information Security Obedience’, as well as the benefits it might hold for an organisation.
8.1 Introduction

The relationship between information security and corporate governance was investigated in Chapter 5. It was concluded from that chapter that the protection of information ultimately contributes to the overall protection of the organisation itself. Therefore, senior management must be responsible for the protection of information through effective information security practices.

Chapter 6 investigated the relationship between corporate governance and corporate culture. The corporate culture largely influences the behaviour of the employees. It was concluded from that chapter that if the senior management can transform the activities of
the employees, the behaviour of the employees will change. As the behaviour changes, it will ultimately transform the culture into one that is in line with senior management’s vision and goals for the organisation.

The relationship between information security and corporate culture was investigated in Chapter 7. It was concluded that employees of an organisation must be aware and have the desire to protect the information in their organisation. This will assist information security practices in becoming an integrated component of the corporate culture of an organisation.

This chapter will investigate the relationship between the three fields of information security, corporate governance and corporate culture. The conclusions of the relationships between the fields discussed in previous chapters will be drawn upon and the term ‘Information Security Obedience’ will be defined.

8.2 Relationship between Information Security and Corporate Governance

The behaviour and actions of employees displayed in their daily work often represent the weakest link in information security practices. Most employees have the necessary privileges to access information and they are often careless with these privileges. Therefore, as indicated in previous chapters, one of the biggest problems facing successful information security practices is the behaviour of employees, represented in Figure 8.1.

![Diagram](image.png)

*Figure 8.1. Information security protection depends on user behaviour and actions*
For employees to be successful in protecting information, it is vital that they know what behaviour is acceptable and unacceptable in terms of information security practices. The question is: who should determine what behaviour is acceptable and unacceptable?

As seen in Chapter 5, senior management, as part of its corporate governance duties, is responsible for the protection of all assets in the organisation. Information is one of an organisation’s most essential assets and the protection of information is critical to the success of an organisation. Senior management is ultimately responsible for the success of the organisation, and, therefore, senior management should be ultimately responsible for the protection of the critical information belonging to the organisation. Senior management must, therefore, outline the vision and direction for information security in the organisation. This responsibility of senior management is shown in Figure 8.2.

![Figure 8.2. Responsibility of senior management for information security](image)

Once the vision and direction for information security has been set by senior management, this commitment should result in the creation of a Corporate Information Security Policy. This Corporate Information Security Policy outlines the vision and goals senior management has for information security, as well as the responsibilities of all employees involved in the organisation. These responsibilities should include what behaviour is acceptable and unacceptable for the protection of information. Figure 8.3 represents this relationship.
Therefore, the Corporate Information Security Policy is a direction-giving document which outlines the procedures required for effective information security practices. In addition, as part of its corporate governance duties, direction-giving is a function of senior management. Therefore, a Corporate Information Security Policy should assist senior management in guiding the organisation in the achievement of information security objectives. In putting a Corporate Information Security Policy in place, senior management also addresses its corporate governance responsibility by ensuring that proper risk management is performed that results in a suitable internal control system. As seen in Chapter 5, protecting the information of an organisation leads to the protection of the organisation itself. This further motivates why senior management should ensure the protection of information.

Thus, it can be concluded from Chapter 5 that to adequately protect an organisation’s information, senior management must outline the vision and direction for information security in the organisation. Senior management must be responsible for the protection of information through the creation of a Corporate Information Security Policy, which details the role employees must play in protecting information. This would assist employees in knowing what behaviour is required from them to protect information. The relationship that should exist between information security and corporate governance is represented in Figure 8.4.
In Figure 8.4, it is seen that management commitment to information security is crucial for an effective relationship between information security and corporate governance. It also shows that to successfully implement information security in an organisation, senior management should create and implement a Corporate Information Security Policy. One of the main functions of senior management is to define the vision for the organisation and guide its organisation in the achievement of this vision. The Corporate Information Security Policy should assist senior management in achieving the vision for information security.

In addition to the role that senior management should play in implementing and sustaining information security in the organisation, they also have a significant role in shaping and transforming the corporate culture in the organisation. The role that senior management plays in shaping and transforming culture is detailed in the following section.

### 8.3 Relationship between Corporate Governance and Corporate Culture

In many organisations, most corporate culture exists by default. In these organisations, no conscious thought or effort is put into shaping the corporate culture into one that would be beneficial and productive for the organisation. Senior management, through its
own actions and behaviour, and through the example it sets, greatly influences the
corporate culture in the organisation. The activities and behaviour of the organisation’s
employees also play a large part in the achievement of the organisation’s goals. The
behaviour of employees is, to a large extent, shaped by the beliefs and values the
employees have at the Shared Tacit Assumptions level of corporate culture. These
beliefs and values influence employees which results in their obvious behaviour found at
the Artifacts level of corporate culture. Therefore, senior management should make a
resolute attempt to shape the Shared Tacit Assumptions level, and, consequently, the
corporate culture into one that will help in the achievement of the organisation’s goals.
The corporate culture ultimately shapes the behaviour of employees, as shown in Figure
8.5.

![Diagram](image.png)

*Figure 8.5. Corporate culture determines employee behaviour*

As part of good corporate governance practices, one of the responsibilities of senior
management is that it must outline the goals and vision for the organisation. These goals
and vision should mirror the espoused values of the organisation and, consequently, is
found at the Espoused Values level of corporate culture. The vision set by senior
management, in the context of corporate governance and corporate culture, is not only
limited to information security, but encompasses the vision for the organisation as a
whole. Figure 8.6 shows that senior management is responsible for setting the vision and
direction for the entire organisation.
Figure 8.6. Senior management outlines the vision for an organisation

It is also senior management’s responsibility to guide the organisation in achieving these goals. Therefore, senior management, as part of its corporate governance duties, should ensure that the necessary elements of corporate culture are in place to support the organisation in achieving its goals. These elements include general management policies. The general management policies of an organisation should outline these goals and vision for the organisation. These policies should outline what activities and behaviour are acceptable and unacceptable for employees when conducting their daily work. This is illustrated in Figure 8.7.

Figure 8.7. The relationship of general management policies

Corporate culture is one of the most established parts of an organisation and is, therefore, not easy to change. The power to change and transform the culture in an organisation is held by senior management. A relationship exists between activities and behaviour and the corporate culture of an organisation. Therefore, if senior management can transform
the activities of the employees, their behaviour will change and it should ultimately transform the culture.

Another factor which influences the behaviour and ultimately the corporate culture is the example set by senior management. In general, employees will model their behaviour on the actions and behaviour of senior management. Therefore, senior management must ensure that its behaviour reflects the general management policies in the organisation. It is also vital for senior management to only accept the behaviour that will benefit the organisation.

The ideal corporate culture would be one where the vision expressed at the Espoused Values level of culture is supported by the actions and behaviour of employees. These actions and behaviour are found at the Artifacts level, which is determined by the Shared Tacit Assumptions level of corporate culture. Therefore, in this ideal culture all three levels of corporate culture would concur. A cultural assessment should be conducted in an organisation to help senior management identify the difference between the current culture and the ideal culture. Senior management, using good corporate governance practices, can then use this difference to attempt to transform the corporate culture into one that will help the organisation attain its goals. The relationship between corporate governance and corporate culture is represented diagrammatically in Figure 8.8.

![Diagram](image)

*Figure 8.8. The relationship between corporate governance and corporate culture*
The relationship depicted in Figure 8.8 shows that it is the behaviour of senior management that, to a large extent, influences the culture in an organisation. The example senior management sets for its employees will have a vast effect on the beliefs and resultant behaviour of its employees. However, it is not only the behaviour displayed by senior management, but also the behaviour they accept from its employees that influences the corporate culture.

General management policies describe what behaviour is acceptable and unacceptable. Senior management must ensure that the policies are implemented in such a way that the behaviour of the employees change, which would ultimately lead to a change in the corporate culture. In order for senior management to do this, it must address the beliefs and values found at the Shared Tacit Assumptions level of corporate culture. Senior management must ensure that its employees’ beliefs will support the espoused values of the organisation.

To achieve senior management's vision it is, in most cases, vital that the information assets of an organisation are protected. Ideally it would be best for the inherent actions and behaviour of employees to reflect the need to protect this information. The following section will detail the importance of information security becoming an essential component in the corporate culture of an organisation.

8.4 Relationship between Information Security and Corporate Culture

Physical and technical controls play an essential role in ensuring effective information security practices. However, it is the cultural and human aspects related to information security that largely determines the sustainability of information security practices. The behaviour of employees towards information is a huge factor in determining the success of information security practices in an organisation. This behaviour is demonstrated at the Artifacts level of culture.
As seen in Chapter 4, the important information assets of an organisation are becoming increasingly accessible to more employees. Therefore, if these employees are not properly aware and informed about acceptable information security practices, they could be the problem when it comes to sustaining information security practices.

An information security awareness program must highlight the significance of protecting the information assets of an organisation. However, the awareness program should not only be used to make employees aware, but to make them fully understand the significance of protecting information and the role they should play in doing this. If employees do not understand the importance of acceptable information security practices, or have the belief that information is not significant to the organisation, they may be apathetic in their information security practices and procedures.

It is, thus, imperative for employees to understand the effect their actions and behaviour have on information security practices and, consequently, the organisation as a whole. Figure 8.1 illustrates the fact that successful information security protection is dependent on user behaviour and actions.

For information security to become an interrelated component of the corporate culture of an organisation, it is crucial that employees have the desire to protect the information of their organisation, and that their behaviour reflects this desire. The employees in an organisation can be the weakest link when it comes to information security practices. However, they can also be the best defense if they are made aware and properly educated about the role they should be playing in the protection of information assets. It is important for information security practices to become a part of the corporate culture of an organisation, so that information security practices become the *de facto* behaviour of the employees. Figure 8.5 illustrates that the corporate culture of an organisation largely determines the behaviour of employees.

The roles that employees should play and the responsibilities they have with regard to information security should be outlined in the Corporate Information Security Policy.
Thus, the Information Security Policy defines what behaviour is acceptable and unacceptable in terms of information security. One of the biggest problems facing information security is the behaviour of employees. Further, the behaviour of employees is largely determined by the corporate culture. Therefore, it follows that the corporate culture of an organisation should be used to shape the behaviour of employees towards effective information security. This can be accomplished with the creation and implementation of a Corporate Information Security Policy, shown in Figure 8.9.

![Diagram](image)

*Figure 8.9. The relationship between information security and corporate culture influenced by a Corporate Information Security Policy*

In order to be successful, information security practices should move out of the conscious thinking of employees and become implicit rules through which information is protected. This would mean that the beliefs and assumptions employees have about information, found at the Shared Tacit Assumptions level, should be positive towards information and employees should have the desire to protect information. If this can be achieved, the Artifacts level of culture, which is directly influenced by the Shared Tacit Assumptions level, would display behaviour that is consistent with good information security practices. Thus, information security becomes part of the overall corporate culture. The relationship between information security and corporate culture is represented diagrammatically in Figure 8.10.
As seen in Figure 8.10, it is the Corporate Information Security Policy that specifies what behaviour employees should engage in to adequately protect information assets. The behaviour of employees is largely influenced by the corporate culture in their organisation. Therefore, the Corporate Information Security Policy should affect the behaviour of employees in such a way that it begins to transform the corporate culture.

The relationships between corporate governance and information security, corporate governance and corporate culture, and information security and corporate culture have been investigated. It is now appropriate to discuss the relationship that exists, or should exist, between the three fields.

### 8.5 Relationships between the Three Fields

The previous section explored the relationships between the fields of corporate governance and information security, corporate governance and corporate culture, and information security and corporate culture. This section will include a table showing the effect the fields have on one another. The term ‘Information Security Obedience’ will then be defined.

Table 8.1 details the effect that unacceptable information security, corporate governance and corporate culture have on one another.
<table>
<thead>
<tr>
<th>Unacceptable</th>
<th>Has an effect on:</th>
</tr>
</thead>
</table>
| **Information Security** | **Corporate Governance:** Senior management must protect all assets of the organisation. Unacceptable information security practices would indicate that information is not properly protected. Therefore, senior management is not fulfilling its corporate governance duties.  
**Corporate Culture:** If there are unacceptable information security practices in an organisation, the result is that the behaviour of employees, which is influenced by the corporate culture, will indicate that information is not protected properly. Therefore, the corporate culture is adversely affected by unacceptable information security practices.  
**Information Security:** Unacceptable corporate governance practices would have an adverse effect on information security practices, as senior management is not properly protecting its information assets. Therefore, unacceptable corporate governance practices have a negative effect on information security practices.  
**Corporate Culture:** Senior management is responsible for guiding its organisation in achieving its goals. Unacceptable corporate governance practices would result in a corporate culture that has no direction or purpose. |
| **Corporate Governance** | **Information Security:** Corporate culture should guide employees in the behaviour that will help an organisation achieve its goals. The result of an unacceptable corporate culture, that does not guide employees in the correct behaviour, will lead to poor information security practices.  
**Corporate Governance:** Senior management must provide guidance for its organisation, which should be reflected in the behaviour of employees (i.e. corporate culture). An unacceptable corporate culture would indicate that senior management is not providing the necessary guidance for its organisation, resulting in poor corporate governance practices. |
| **Corporate Culture** | **Table 8.1** Effects of unacceptable information security, corporate governance and corporate culture. |
Table 8.2 details the effect that acceptable information security, corporate governance and corporate culture have on one another.

<table>
<thead>
<tr>
<th>Acceptable</th>
<th>Has an effect on:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Information Security</strong></td>
<td>Corporate Governance: Senior management must protect its organisation through the protection of assets. Acceptable information security practices result in the vital asset of information being protected, which indicates that senior management has fulfilled its corporate governance duties with regard to information.</td>
</tr>
<tr>
<td><strong>Corporate Governance</strong></td>
<td>Corporate Culture: If acceptable information security practices are in place in an organisation, it indicates that the behaviour of employees is protecting information. If the behaviour of employees protects information it will ultimately change the corporate culture, and the behaviour of employees will become second-nature. Therefore, acceptable information security practices should have a positive effect on the corporate culture.</td>
</tr>
<tr>
<td><strong>Corporate Culture</strong></td>
<td>Information Security: One of the main functions of senior management, as part of its corporate governance duties, is to protect the assets of its organisation. Therefore, if there are acceptable corporate governance practices in place, it indicates that information assets are protected. Acceptable corporate governance practices, therefore, results in acceptable information security practices.</td>
</tr>
<tr>
<td><strong>Corporate Culture</strong></td>
<td>Corporate Culture: Acceptable corporate governance practices indicate that senior management is in control of the organisation, and should be taking an active role in shaping the corporate culture. Therefore, acceptable corporate governance practices should result in a corporate culture that helps an organisation achieve its goals.</td>
</tr>
</tbody>
</table>
Corporate Governance: If the corporate culture, and the resulting behaviour of employees, is beneficial to the organisation and assisting the organisation in achieving its goals, then it should result in acceptable corporate governance practices. This is because one of the aims of good corporate governance is the achievement of the goals of the organisation.

Table 8.2  Effects of acceptable information security, corporate governance and corporate culture.

From the tables it can be concluded that, whether acceptable or unacceptable, information security, corporate governance and corporate culture all have an effect on one another.

In Chapters 2, 3 and 4 of this dissertation the three fields of information security, corporate governance and corporate culture have been investigated individually. Chapters 5, 6 and 7, and previous sections of this chapter, explored the relationships between corporate governance and information security, corporate governance and corporate culture, and information security and corporate culture. The previous figures in this chapter can be combined into one figure that represents all relationships between the three fields, as detailed in this chapter. This combination is represented by Figure 8.11.
Figure 8.11. The relationships between information security, corporate governance and corporate culture

The relationship that should exist between information security and corporate governance, represented by ‘A’ in the figure, is highlighted with the following quote from Michael Cangemi, President of the Etienne Aigner Group Inc. He states that, ‘The information possessed by an organisation is among its most valuable assets and is critical to its success. The Board of Directors, which is ultimately accountable for the organisation's success, is therefore responsible for the protection of its information. The protection of this information can be achieved only through effective management and assured only through effective board oversight’ (March 2000, online). This highlights the fact that there should be a very strong relationship between the fields of information security and corporate governance.

As detailed previously, information security is currently seen as an overhead, and not as an investment. The senior management of an organisation tends to view information security as a technical problem that the Information Technology department should be concerned with. However, the information that resides on an organisation’s systems is owned by the organisation as a whole, not the IT manager. Therefore, it is the senior management of organisations that needs to direct the approach to protecting the information.

Senior management must indicate exactly what it expects from its employees as far as information security is concerned. Employees require guidelines and direction for information security practices to shape their behaviour and actions. The Corporate Information Security Policy can address both these issues. Thus, one of the best ways to develop the relationship between information security and corporate governance is for senior management to implement and sustain information security practices through the
Corporate Information Security Policy. Therefore, the Corporate Information Security Policy should play a critical role in the way that senior management governs the security of information.

The relationship, represented by ‘B’ in the figure, represents the relationship between information security and corporate culture. When investigating information security, it is often seen that the procedures that employees use in their daily work and their behaviour could symbolise the weakest link in information security. In addition, it has been pointed out that the corporate culture of an organisation, to a large extent, determines the behaviour and actions of employees. Therefore, the corporate culture in an organisation should be used to influence the behaviour of the employees towards information security in a positive way. Understanding the corporate culture in terms of information security is crucial, and assessing employees’ awareness, competence and commitment determines the best method for the implementation and distribution of the Corporate Information Security Policy.

This Corporate Information Security Policy must outline the behaviour expected from employees with regard to protecting information. Employees must adhere to this acceptable behaviour, which should then begin shaping the corporate culture into one that is more security conscious. A Corporate Information Security Policy should assist in cultivating a corporate culture in which the actions and behaviour of employees are in line with the policy. Therefore, as information security is highly dependent on the behaviour of the users of information, the behaviour should preferably be instilled through corporate culture to ensure that acceptable behaviour becomes the de facto behaviour.

The relationship between corporate governance and corporate culture is represented by ‘C’ in the figure. As detailed in section 8.3, this relationship is one where senior management should create general management policies using effective corporate governance strategies. These policies should play a primary role in shaping the culture in the organisation by specifying the acceptable and unacceptable behaviour for the
employees. These guidelines are crucial in cultivating a beneficial corporate culture. However, the culture in an organisation is not determined solely by what management stipulates in the policies, but rather what management accepts in practice.

Therefore, the behaviour senior management accepts in the organisation should be the behaviour outlined in management policies. Thus, the power to change the corporate culture in an organisation is held by senior management. The policies created by senior management should alter the behaviour of the employees in an organisation and should, therefore, start to influence the corporate culture in that organisation. Therefore, as information security is a management responsibility, the Corporate Information Security Policy should guide employees to behave in a way that ensures the protection of information.

The relationship represented by ‘D’ in the figure represents the incorporation of all three fields of corporate governance, information security and corporate culture. Corporate culture, to a large extent, determines the actions and behaviour of the employees of an organisation. As seen in this chapter, the power to change the corporate culture of an organisation resides, to a large extent, with senior management. Therefore, senior management should be able to transform the behaviour of the employees in the organisation into behaviour that will benefit the organisation. As it is the behaviour of employees that is often the weakest link in information security practices, senior management should be able to transform the behaviour of employees into behaviour that will promote proper information security practices. Ideally, to protect information, the de facto behaviour of employees should reflect the desire to protect information. In other words, the Shared Tacit Assumptions level of culture, which influences the Artifacts level of culture, should be aligned with the Espoused Values level of corporate culture. In order to achieve this, senior management should implement a Corporate Information Security Policy that outlines the behaviour that employees should display in protecting information assets. The behaviour detailed in the Information Security Policy should reflect the behaviour that senior management accepts as conducive to the well-being of the organisation.
The relationship between these three fields can be encapsulated by a single term proposed in this dissertation. This relationship between the three fields and the term used to encompass all three fields will be discussed in the following section.

8.6 Information Security Obedience

This section will investigate the relationship between all three fields of information security, corporate governance and corporate culture. To be successful, information security needs to become part of the way the employees conduct their daily tasks, from senior management, right throughout the entire organisation. Therefore, information security should become an intricate part of the corporate culture of the organisation, as it is the culture that determines how employees conduct their daily tasks. This relationship should represent the situation whereby senior management’s vision for the protection of information in the organisation is conveyed through the Corporate Information Security Policy. This policy should be drafted, advocated and implemented in such a way that it positively influences the corporate culture with regard to information security. Further, as information security is highly dependent on the correct behaviour of users, the corporate culture should contribute towards the fact that the de facto behaviour of users is indeed what senior management envisaged as acceptable behaviour.

This relationship can be encompassed by the term ‘Information Security Obedience’. In assessing the acceptability of the term ‘Information Security Obedience’, numerous people expressed concern over the negative connotations associated with the term ‘obedience’. The perception is that when using the term ‘obedience’, a ‘master’/‘slave’ relationship exists, where employees would be forced to submit to the authority of senior management. This, however, is not the case, as is detailed in the following paragraphs.

Obedience is defined as ‘compliance with that which is required by authority’ (Dictionary.com, 2003, online). The authority in this case is the senior management of organisations, striving towards effective corporate governance. Senior management should create a Corporate Information Security Policy to outline exactly what employees
should comply with. Another definition is, ‘words or actions denoting submission to authority’ (Dictionary.com, 2003, online). These words or actions translate into the practices and behaviour of employees, which senior management should have deemed acceptable or unacceptable. As detailed previously, the practices and behaviour of employees are, to a large extent, determined by the corporate culture in an organisation.

Therefore, by using the term ‘Information Security Obedience’, it binds together all three fields of information security, corporate governance and corporate culture. The term does this by stating that the actions of the employees must comply with that which is required by senior management in terms of information security. ‘Information Security Obedience’ is not something that should be forced on the employees of an organisation, but should rather become part of the overall corporate culture. Therefore, ‘Information Security Obedience’ is defined, for the purposes of this dissertation, as ‘de facto user behaviour complying with the vision of senior management as defined in the Corporate Information Security Policy’.

8.7 Conclusion

Senior management is ultimately responsible for the protection of all assets in the organisation. Therefore, as seen in this chapter, the relationship that should exist between corporate governance and information security is one where the senior management of an organisation must be responsible for the protection of the information assets of the organisation. This protection should be achieved through information security risk management and internal control, resulting in a Corporate Information Security Policy implemented and enforced in the organisation.

Also seen was the relationship between corporate governance and corporate culture. The corporate culture of an organisation is largely influenced by the behaviour displayed and accepted by senior management. If the management policies of an organisation specify certain actions and behaviour, but senior management accepts different actions and behaviour from its employees, these employees will usually behave according to what management accepts rather than what the policy specifies. Therefore, senior
management has the power to transform the corporate culture in the organisation, accepting only the behaviour that will benefit the organisation. The behaviour that senior management accepts should be detailed in the management policies.

This chapter also described the relationship between information security and corporate culture. The behaviour of employees towards information assets is often the weakest link in information security practices. As it is the corporate culture that greatly influences the behaviour of employees, it follows that to positively affect the behaviour of employees towards information security the corporate culture must be transformed. Information security practices should become part of the corporate culture of an organisation to be truly effective. As it is policies that describe what behaviour is acceptable and unacceptable, the Corporate Information Security Policy should be used to positively affect the behaviour of employees towards information security.

‘Information Security Obedience’ describes the relationship that should exist between the fields of corporate governance, information security and corporate culture. ‘Information Security Obedience’ states that the actions and behaviour that employees display in information security practices should become second-nature to the employees. This behaviour must be the behaviour that is condoned and accepted by senior management. In addition, this behaviour must be outlined in the Corporate Information Security Policy. This behaviour must assist the organisation in achieving the vision defined by senior management. ‘Information Security Obedience’ should be an objective for an organisation. This objective can be achieved through an acceptable Corporate Information Security Policy, associated with acceptable education and awareness, assisted by a correct example from senior management.
9.1 Introduction

The previous chapters in this dissertation explored the three fields of information security, corporate governance and corporate culture. All three fields are vital in the daily operation of a successful organisation. Good corporate governance practices should be employed by the senior management of an organisation. Corporate culture moulds the behaviour of employees in an organisation. Effective information security practices are necessary for the protection of information assets.

The following section contains a summary of the material that was explored in the previous chapters.
9.2 Summary

Chapter 1 introduced the fields of information security, corporate governance and corporate culture. It outlined how important these fields are for the success of an organisation and the importance of relating these fields to one another. The problem statement, as well as the objectives, for the dissertation was defined and the methodology used towards the solution to this problem statement was outlined.

An increasing number of organisations admit to having sensitive information that is critical to the organisation. This sensitive information should be protected using effective information security mechanisms and practices. Information security was investigated in Chapter 2. Effective information security practices should ensure that the three pillars of information security; confidentiality, integrity and availability, are well preserved. It was highlighted in this chapter that inadequate information security practices can be devastating for an organisation. One of the biggest problems facing effective information security practices is the behaviour and actions of employees. Traditionally, physical and technical controls were regarded as the most important controls for the protection of information, but currently it is the operational controls, dependent on employee behaviour, that sustain information security practices.

The field of corporate governance was investigated in Chapter 3. The importance of corporate governance and the threats to the field were discussed, as well as the four essential pillars required for effective corporate governance practices in an organisation. One of the main aims of the Board of Directors should be to ensure that the various policies and procedures that are required to protect the organisation’s assets and resources are in place. Senior management, using proper corporate governance practices, must ensure that these policies and procedures of the Board are effectively implemented and practiced in the organisation. Thus, senior management must set and communicate the vision and direction for effective information security to the employees, as well as how it expects the employees to behave when working with information assets.
Corporate culture exists at three levels. The Artifacts level of culture displays the visible behaviour of employees. This level is directly influenced by the Shared Tacit Assumptions level which represents the common beliefs and values of employees. These levels, together with the Espoused Values level, were explored in Chapter 4. Corporate culture was defined and the origins of a culture were also explored. The deepest level of corporate culture, the Shared Tacit Assumptions level, directly influences the behaviour of employees. Therefore, the corporate culture shapes the behaviour of the employees in an organisation. Thus, the behaviour of employees can be changed by transforming the corporate culture.

One of the challenges facing information security is the adverse perception of senior management that information security is a technical issue and, therefore, not one of its main concerns. Chapter 5 explored the relationship that should exist between information security and corporate governance. As part of senior management’s corporate governance duties it must protect the assets of the organisation through a risk management process complemented by a related internal control system. One of these assets is information. The Corporate Information Security Policy must detail the role employees should play in protecting the information in the organisation. It is senior management’s responsibility to ensure that the policy is drafted and implemented to ultimately affect the behaviour of employees positively towards information security.

The factors that help shape the corporate culture and the influence that management policies have on the corporate culture were explored in Chapter 6. The relationship between corporate governance and corporate culture was investigated. Cultural assessment should play a role in helping senior management determine what needs to be done in the organisation to achieve its vision. The ability of senior management to effect and transform the corporate culture into one that will benefit the organisation was also investigated. Senior management can shape the corporate culture of the organisation by setting an example to the rest of the employees and only accepting behaviour that will help in the achievement of its vision.
To be truly effective, information security should become an intricate part of the corporate culture in an organisation. Chapter 7 explored the relationship that should exist between information security and corporate culture. Acceptable employee behaviour is vital in ensuring the success of information security practices. As it is the corporate culture that largely determines the behaviour of employees, it follows that information security practices should become part of the corporate culture. The Corporate Information Security Policy should assist in the integration of corporate culture and information security, as it describes the behaviour and actions employees should use in protecting information assets.

Chapter 8 explored the relationship between all three fields of information security, corporate governance and corporate culture, and the term ‘Information Security Obedience’ was defined. This term detailed that good information security practices should become second-nature to the employees of an organisation by becoming part of the corporate culture. The practices should assist in the achievement of the vision set out by senior management for information security.

9.3 Solving the Problem

The problem statement of this dissertation stated that for information security practices to be effective, widespread human involvement is required. This human involvement is in the form of behaviour and actions required for an effective internal control system to ensure the successful protection of information. Employees must know what behaviour is acceptable in their organisation. However, in most cases, employees have no guidance and direction in terms of acceptable behaviour as far as information security practices are concerned.

This acceptable behaviour should be detailed and clearly spelt out by senior management, as part of good corporate governance practices. The dissertation highlighted the critical role that the Corporate Information Security Policy plays in detailing this acceptable
behaviour. The Corporate Information Security Policy allows senior management to set its vision and direction for appropriate information protection and to provide support. The Corporate Information Security Policy, supported by proper procedures, should also provide the necessary guidance to employees to act and behave in such a way that a high level of information security is ensured. Thus, as motivated in this dissertation, the Corporate Information Security Policy should provide the ‘glue’ that links information security and corporate governance together.

In prescribing acceptable behaviour and actions to the users of information, the ideal would be if this correct behaviour became second-nature to the employees. The dissertation also motivated that this can be done through the cultivation of a corporate culture that is conducive to maintaining a high level of information security. The Corporate Information Security Policy should assist in cultivating this culture by changing the common beliefs and values of employees, and, thereby, shaping the behaviour and, ultimately, the corporate culture of an organisation. The role of senior management in cultivating such a corporate culture was also identified and detailed.

Thus, the relationship and integration of these three very important fields have been motivated and argued and in doing so, all the set objectives as listed in section 1.3 have been met.

### 9.4 Further Research

Senior management must detail its vision for information security in the Corporate Information Security Policy. The Corporate Information Security Policy must also provide guidelines for the actions and behaviour of employees when protecting information. This policy must influence the Shared Tacit Assumptions level of corporate culture in order to change the behaviour of employees towards information assets.

Therefore, the Corporate Information Security Policy is vital in ensuring information security practices become *de facto* behaviour for employees. However, precisely how the Corporate Information Security Policy should be drafted and communicated to achieve
this has not been addressed in this dissertation. This should be addressed in a further research project.

The fact that corporate culture plays a large role in creating acceptable behaviour has also been motivated. Senior management, through the example it sets, also plays an important part in defining acceptable behaviour. However, precisely how information security awareness and education should be conducted to successfully create a corporate culture that supports information security practices must also be researched further.

Thus, it has been realised that the Corporate Information Security Policy, the associated security awareness and education and the example and influence of senior management all contribute to a state of ‘Information Security Obedience’. The factors required for ‘Information Security Obedience’ and exactly how a state of ‘Information Security Obedience’ can be achieved should be investigated in further research.

9.5 Conclusion

Information is a vital asset in most organisations and as such should be well protected through effective information security practices. One of the problems facing the protection of information is the actions and behaviour of the employees in an organisation. If information security practices could become second-nature to employees and part of the way they conduct their daily activities, it would, to a large extent, eliminate this problem.

The behaviour of employees is largely determined by the corporate culture in their organisation. Therefore, in order to change the behaviour of employees, the corporate culture of an organisation should be transformed into one that will benefit the information security practices.

Corporate culture is one of the most stable components of an organisation. However, senior management has the ability to transform the corporate culture in the organisation. A vital pillar for corporate governance is responsibility and one of the main
responsibilities of senior management is to define the vision for the organisation and strive towards the achievement of this vision. The activities, culture and vision of an organisation are interrelated. Culture shapes the activities and behaviour of employees and ultimately the corporate culture, which should assist in attaining the vision of senior management.

Another responsibility of senior management is the protection of important assets of the organisation. Information is a critical asset in most organisations and the success of an organisation could be largely dependent on the protection of information. Therefore, as part of senior management’s overall vision for the organisation, the vision for information security must be outlined.

In order to change the corporate culture of an organisation, the three levels of culture must be addressed. Senior management should address the Espoused Values level of culture through its management policies. One of these policies should be the Corporate Information Security Policy which should describe what is required in an organisation to effectively protect information. Key to the Information Security Policy should be the role employees play and the behaviour they should demonstrate in protecting information. However, the Artifacts level of culture, which displays the visible behaviour of employees, will not reflect the necessary behaviour to protect information outlined at the Espoused Values level if the Shared Tacit Assumptions level of employees is not addressed.

The Shared Tacit Assumptions level of culture consists of all the shared beliefs and values of employees. This level directly influences the visible behaviour of employees at the Artifacts level. Therefore, for senior management to change the behaviour of employees, with regard to information security practices, it must address the values and beliefs (Shared Tacit Assumptions) that employees have about information security.

Senior management must ensure that the Shared Tacit Assumptions level of culture, in terms of information security, is in line with the information security vision defined at the
Espoused Values level of culture. To accomplish this change in corporate culture, senior management must set an example for the rest of the organisation by emphasising the importance of information security and displaying good information security practices. The behaviour senior management accepts from the employees will also determine the ultimate actions of employees.

For senior management to change the beliefs and values of its employees with regard to information security, an information security awareness program must aim to, not only, make employees aware of information security, but also ensure they fully understand the impact of their actions in protecting information assets. The Corporate Information Security Policy must also be implemented in an organisation so that employees understand their role in information security practices and the consequences associated with not adhering to these practices.

In this way, information security practices, driven by senior management using good corporate governance practices, should become second-nature to employees and part of the overall corporate culture in an organisation. The term to encompass this relationship between information security, corporate governance and corporate culture is ‘Information Security Obedience’ - ‘de facto user behaviour complying with the vision of senior management as defined in the Corporate Information Security Policy’.
References


Appendix A1: Papers Presented and Published

**Paper 1**
In May 2003, at the 18th IFIP International Information Security Conference held in Athens, Greece, Kerry-Lynn presented the paper ‘Integrating Information Security into Corporate Governance’.

This paper investigated the relationship between information security and corporate governance and the role the Board of Directors should play in protecting information. This paper detailed that information security is a direct management concern, as the Board should be responsible to the shareholders of the organisation and accountable to a court of law.

**Paper 2**
In July 2003, at the ISSA Conference held in Johannesburg, South Africa, Kerry-Lynn presented the paper ‘Creating a Security Conscious Culture through Effective Corporate Governance’.

This paper outlined the important role that a Corporate Information Security Policy should play in securing information. The paper detailed that senior management should be responsible for the creation of this Information Security Policy and should outline the role that employees of an organisation should play in protecting information.

**Paper 3**
Currently, the paper ‘Information Security Obedience: A Definition’ is under review for publication in the *Computers & Security* journal.

This paper detailed that one of the biggest problems facing information security is the behaviour of employees. The paper detailed that the Corporate Information Security Policy should outline the vision and goals for information security, and should influence the behaviour of employees. The paper also defined the term ‘Information Security Obedience’.
Appendix A2: Article

INFORMATION SECURITY OBEDIENCE: A DEFINITION

Kerry-Lynn Thomson\textsuperscript{a} and Rossouw von Solms\textsuperscript{b}

\textsuperscript{a}Port Elizabeth Technikon, South Africa
\textsuperscript{b}Port Elizabeth Technikon, South Africa

\textsuperscript{a}kthomson@petech.ac.za, Department of Information Technology, PE Technikon, Private Bag X6011, Port Elizabeth 6000
\textsuperscript{b}rossouw@petech.ac.za, Department of Information Technology, PE Technikon, Private Bag X6011, Port Elizabeth 6000

Abstract
Information is a fundamental asset within any organisation and the protection of this asset, through a process of information security, is of equal importance. This paper examines the relationships that exist between the fields of corporate governance, information security and corporate culture. It highlights the role that senior management should play in cultivating an information security conscious culture in the organisation, for the benefit of the organisation, senior management and the users of information.

Key Words
Corporate Governance, Information Security, Corporate Culture, Information Security Obedience
INFORMATION SECURITY OBEDIENCE: A DEFINITION

1. INTRODUCTION

Information is important. It is often depicted as the lifeblood of the growing electronic economy (Gordon, 2002, online). Commercial organisations and governments rely heavily on information to conduct its daily activities. Therefore, the security of information needs to be managed and controlled properly (Lane, 1985, pp 2-3; Smith, 1989, p 193). No matter what the information involves; whether it is customer records or confidential documentation, there are many threats that make information vulnerable (Gordon, 2002, online). Information security, therefore, needs to be implemented and managed within the organisation to ensure that the information is kept safe and secure (Krige, 1999, p 7).

Information is an organisational asset, and consequently the security thereof needs to be integrated into the organisation’s overall management plan (Lane, 1985, pp 2-3; Smith, 1989, p 193). Effective corporate governance should dictate this overall management plan. Sir Adrian Cadbury, in the foreword of Corporate Governance: A Framework for Implementation has the following description of corporate governance. He states that corporate governance deals with establishing a balance between economic and social goals and between individual and mutual goals. The framework for governance is there to promote the competent use of resources and, in the same way, to involve accountability for the stewardship of those resources (World Bank Group, 1999, online).

It is inevitable that these organisations that should deploy effective corporate governance develop a corporate culture. Cultural assumptions in organisations develop around how people in the organisation relate to one another, but that is only a tiny portion of what culture covers (Schein, 1999, p 28). Corporate culture is generally defined as values that are shared by everyone in an organisation, including fundamental beliefs, principles and practices (Beveridge, 1997, online). These fundamental beliefs, principles and practices
have a direct influence on the behaviour patterns of employees as far as information security is concerned.

The purpose of this paper is to investigate to what extent the senior management of an organisation should be involved in changing the beliefs, principles and practices of its employees towards information security, thereby influencing their behaviour favourably towards the protection of information. The paper will initially investigate the field of corporate governance, followed by the challenges facing corporate governance and information security. Corporate culture and its importance to an organisation will then be explored and the paper will conclude by investigating the relationships between information security, corporate governance and corporate culture. Based on this investigation, the term ‘Information Security Obedience’ will be defined.

2. CORPORATE GOVERNANCE

Corporate governance is a contemporary term for an issue which has been challenging organisations for decades – that of ‘accountability’. Corporate governance is defined as the exercise of power over and responsibility for corporate entities (Blackwell Publishers, 2000, online). At its most fundamental level, corporate governance provides assurance that an organisation has the necessary corporate structures to support accountability (Brooks, 1997, online).

Accountability, however, is only one of the four pillars of corporate governance. The remaining pillars are responsibility, fairness and transparency (King Report, 2001, p 17; World Bank Group, 1999, online). The pillar of *accountability* ensures that individuals or groups in an organisation are accountable for their decisions and actions (King Report, 2001, p 14). The second pillar, *responsibility*, indicates that corrective action can be taken against mismanagement and misconduct (King Report, 2001, p 14). *Fairness*, the third pillar of corporate governance, attempts to ensure that there is a balance in an organisation. The rights of various groups should be recognised and valued (King Report, 2001, p 14). The final pillar, *transparency*, is the ease with which outsiders can see what is transpiring inside an organisation (King Report, 2001, p 13).
Through these corporate governance pillars, the Board of Directors is both accountable and responsible to the organisation and its shareholders for the wellbeing of the organisation (King Report, 2001, p 17). Information is a vital asset to most organisations, and because the Board of Directors is both accountable and responsible for the welfare of the organisation they should ensure that the organisational asset of information is protected to ensure the well-being of the organisation (Deloitte & Touche, 2002, online).

3. CHALLENGES FACING CORPORATE GOVERNANCE AND INFORMATION SECURITY

There are many challenges facing the convergence of corporate governance and information security – one of which is to convince the senior management of an organisation that it should be ultimately accountable and responsible for the protection of its organisation’s information. PriceWaterhouseCoopers highlights the lack of support there is for information security, in their 2002 Information Security Breaches Survey, by stating that ‘The root cause is that security is treated as an overhead rather than an investment’ (PriceWaterhouseCoopers, 2002, p 3).

Furthermore, according to PriceWaterhouseCoopers, only 27% of organisations in the United Kingdom spend more than 1% of their Information Technology budget on protecting their information and only 5% of organisations spend more than 10% of their IT budget on information security (PriceWaterhouseCoopers, 2002, p 3). This lack of attention to information security could be as a result of the fact that managers can normally only allocate a limited amount of time and consideration to information security. As a consequence, management’s attention is often limited to a small group of acute threats and countermeasures that happen to relate to the issues of the day (Buren, van der Meer, Shahim, Barnhoorn & Roos Lindgreen, 1999, p 76).

However, the successful operation of organisations today relies on information, and the exchange of information. Further, the protection of information, through information security, is important for the impact it can have on business (Deloitte & Touche, 2002, online).
online). Therefore, management should be concerned with information security as information is vital for the success of the organisation. In fact, they are accountable and responsible for the well-being of the organisation that depends heavily on information, as highlighted earlier.

One of the ways for management to demonstrate its dedication to information security in the organisation is to provide the support and commitment towards a formally agreed upon and documented Corporate Information Security Policy, as it is one of the controls that is considered common best practice in terms of information security (BS 7799-1, 1999, p 4).

Quality information security begins and ends with quality management policies (Whitman & Mattord, 2003, p 194). An overriding duty of the Board of Directors is to ensure the long-term feasibility of an organisation. To do this, it is essential that the assets of an organisation are protected (World Bank Group, 1999, online).

Therefore, it follows that the Board of Directors should be involved in the protection of information, an important organisational asset. The level of information security that the Board of an organisation is prepared to propose and put into operation, and the level of information security that is acceptable to the shareholders should be consolidated and result in the Corporate Information Security Policy (King Report, 2001, p 96). The Information Security Policy should be based on the approved corporate security objectives and strategy and is there to provide management direction and support for information security (British Standards Institute, 1993, p 17).

The main aim of any policy, whether for information security or not, is to influence and determine decisions, actions and other issues, by specifying what behaviour is acceptable and what behaviour is unacceptable. Policies and procedures are, therefore, organisational laws that determine acceptable and unacceptable conduct within the context of corporate culture (Whitman & Mattord, 2003, p 194).
4. CORPORATE CULTURE

Every organisation has a culture and this culture exists at both a conscious and unconscious level (Hagberg Consulting Group, 2002, online). This culture could be operating with authoritative principles and driven by top management. However, many organisations have a culture that exists by default. This culture changes by accident and is influenced by a few key people in the organisation (Atkinson, 1997, p 16). A disturbing fact is that it is estimated that only 5% of organisations have a definable culture, where the senior management takes an active role in the shaping of the culture (Atkinson, 1997, p 17). If management does not understand the culture in the organisation, it could prove to be fatal in today’s business world (Hagberg Consulting Group, 2002, online).

Culture is the overall, taken-for-granted assumptions that a group has learned throughout history (Schein, 1999, p 29). Corporate culture is an extensive issue and because the shared beliefs of an organisation include values about what is desirable and undesirable – how things should and should not be – these beliefs dictate the kinds of activities that are ‘legal’ and the kinds that are ‘illegal’ for the employees in an organisation (Beyer, 1981, p 21).

Since corporate culture plays a major role in the actions of employees in an organisation, it is an important aspect in an organisation, as it is central to restraining or enhancing the performance of an organisation (Atkinson, 1997, pp 16-17). Culture is imperative because it is a powerful, underlying and often unconscious set of forces that establishes individual and group behaviour. Corporate culture is especially important because cultural elements determine the strategy and goals of an organisation (Schein, 1999, p 14).

One of the difficulties in trying to understand culture is that it is a very complex discipline, which should not be oversimplified. It is very simple to say that culture ‘is the way things are done around here’, but a much better way of thinking is to appreciate that culture exists at numerous levels. These levels range from the visible to the tacit and
invisible. Furthermore, it is imperative that these levels are managed and understood (Schein, 1999, p 15).

Levels of Corporate Culture

The corporate culture and behaviour of people in organisations has been extensively researched by Edgar H. Schein. Schein states that, ‘A better way to think of culture is to realise that it exists at several ‘levels’, and that we must understand and manage the deeper levels’ (1999, p 15).

The first level of corporate culture and probably the simplest level to examine in an organisation is that of artifacts. Some of the most visible expressions of culture are these artifacts (Hagberg Consulting Group, 2002, online). Artifacts can be described as what an individual can see, hear and feel when they walk into an organisation. Examples of artifacts could range from the design and décor of the organisation to how people behave towards each other and customers (Schein, 1999, p 16).

Espoused values are the second level of culture in an organisation. These are the values expressed and published in an organisation’s policies and are those values that an organisation is said to be promoting. Examples of espoused values are teamwork and good communication (Schein, 1999, p 17).

When it comes to the first two levels of corporate culture, there could be a few obvious contradictions between some of the espoused values or goals of an organisation and the visible behaviour of an organisation as seen at the artifacts level. What these contradictions between the two levels indicate is that a deeper level of thought and insight is driving the evident behaviour of the employees (Schein, 1999, p 18). What an organisation strives to do and the values it wishes to endorse may be different from the values, beliefs, and norms expressed in the actual practices and behaviour of the organisation (Hagberg Consulting Group, 2002, online). Therefore, the deeper level that drives the visible behaviour may or may not be consistent with the values and principles that are espoused by the organisation. So, to truly understand the culture of an
organisation the deepest level of corporate culture must be understood (Schein, 1999, pp 18-19).

Schein refers to this deepest level as the *shared tacit assumptions* level. The heart of corporate culture is the mutually learned values, beliefs and assumptions that have become taken for granted as the organisation continues to be successful. These tacit assumptions involve the nature of the organisation’s environment and how to succeed in it. Examples of shared tacit assumptions are unique to a particular organisation, but generally are decisions and actions that are second-nature to an employee (Schein, 1999, p 19).

Therefore, the decision and actions of employees are determined through the three levels of corporate culture. And these three levels emphasise that culture is extremely stable, as it represents the accumulated learning of a group (Schein, 1999, p 21).

As has been highlighted earlier, the Board of Directors should be both accountable and responsible for the well-being of an organisation which depends on information and information resources. To protect this information, the behaviour patterns of employees must assist in ensuring information security. Since, the corporate culture of an organisation determines the behaviour of employees in an organisation; it should be used to influence these behaviour patterns of employees towards the protection of information as envisioned by the Board of Directors.

5. **RELATIONSHIPS BETWEEN THE THREE FIELDS**

The three fields of information security, corporate governance and corporate culture have been highlighted individually in the earlier part of the paper. The following section will investigate the relationships that should exist between these three fields. The relationships between the fields can be depicted diagrammatically, as shown in Figure 1.
The relationship that should exist between information security and corporate governance, represented by ‘A’ in the diagram, is highlighted with the following quote from Michael Cangemi, President and COO of the Etienne Aigner Group Inc. He states that, ‘The information possessed by an organisation is among its most valuable assets and is critical to its success. The Board of Directors, which is ultimately accountable for the organisation's success, is therefore responsible for the protection of its information. The protection of this information can be achieved only through effective management and assured only through effective board oversight’ (IIA, AICPA, ISACA, NACD, March 2000, online). This highlights the fact that there is a very strong relationship between the fields of information security and corporate governance.

As seen in previous sections of the paper, information security is currently being seen as an overhead, rather than as an investment. The senior management of organisations tends to view information security as a technical problem that the IT department should be concerned with. However, the information that resides on an organisation’s systems is owned by the business as a whole, not the IT manager. Information and information
systems play critical roles in business processes. Therefore, it is the senior management of organisations that needs to direct the approach to protecting the information (Deloitte & Touche, 2002, online). Proactively addressing an organisation’s information security issues in the digital era is not only good business practice; it is a necessity (Gordon and Glickson, 2001, online). One of the ways to enhance the relationship between information security and corporate governance is for senior management to support and direct the creation and implementation of a Corporate Information Security Policy. Therefore, the Corporate Information Security Policy should play a critical role in the way that senior management governs the security of information.

The relationship, represented by ‘B’ in the diagram, represents the relationship between information security and corporate culture. When investigating information security, it is often seen that the procedures employees use in their daily work and their behaviour could symbolise the weakest link in information security (Martins and Eloff, 2002, p 203). In addition, it has been pointed out that the corporate culture of an organisation, to a large extent, determines the decisions and actions of employees (Schein, 1999, p 17).

Therefore, the corporate culture in an organisation should be used to influence the behaviour of the employees towards information security in a positive way. In order to do this, the shared tacit assumptions level of corporate culture must be addressed. The collective beliefs and values of employees are found at this level of corporate culture. This shared tacit assumptions level directly influences the artifacts level of culture, which displays the visible behaviour of employees.

Therefore, for employee behaviour to change; their beliefs must be altered positively towards information security. Understanding the corporate culture around information security is crucial, and assessing employees’ awareness, competence and commitment determines the best method for the implementation and distribution of the Corporate Information Security Policy so that it will be effective (Deloitte & Touche, 2002, online). An encompassing Information Security Policy should assist in cultivating a corporate culture that takes advantage of the benefits of information security practices (Gordon and
Glickson, 1997, online). Therefore, as information security is highly dependent on the behaviour of the users of information, the behaviour should preferably be instilled through corporate culture to ensure that acceptable behaviour becomes the de facto behaviour.

The relationship between corporate governance and corporate culture is represented by ‘C’ in the diagram. The behaviour of employees is, to a large extent, shaped by the beliefs and values the employees have at the shared tacit assumptions level of corporate culture. Therefore, senior management should make a resolute attempt to shape the shared tacit assumptions level, and, consequently, the corporate culture into one that will help in the achievement of the organisation’s goals.

As part of good corporate governance practices, one of the responsibilities of senior management is that it must outline the goals and vision for the organisation. These goals and vision of an organisation should be what is expressed by senior management at the espoused values level of corporate culture. It is also senior management’s responsibility to guide the organisation in achieving these goals. Therefore, senior management, as part of its corporate governance duties, should ensure that the necessary elements of corporate culture are in place to support the organisation in achieving its goals.

The ideal corporate culture would be one where the vision expressed at the espoused values level of culture by senior management is supported by the actions and behaviour of employees determined by the shared tacit assumptions level of corporate culture.

The behaviour displayed by senior management, in terms of information security practices, helps shape the attitude of employees towards information security. In addition, it is also the behaviour senior management accepts from the employees that influences the corporate culture. Management policies describe what behaviour is acceptable and unacceptable. Senior management must ensure that the policies are implemented in the organisation in such a way that the behaviour of the employees changes, which would ultimately lead to a change in the corporate culture. Therefore, as information security is a management responsibility, the Information Security Policy
should guide employees to function in a manner that adds to the protection of information (Whitman & Mattord, 2003, p 194). As detailed previously, for senior management to transform the corporate culture in the organisation they must address the beliefs and values found at the shared tacit assumptions level of corporate culture. Senior management must ensure that the employees’ beliefs will support all espoused values of the organisation, including the vision for information security.

The relationship represented by ‘D’ in the diagram is the relationship between the three fields of information security, corporate governance and corporate culture. To be genuinely valuable, information security needs to become part of the way everyone conducts their daily tasks, from senior management, throughout the entire organisation (Deloitte & Touche, 2002, online). Therefore, information security should become an intricate part of the corporate culture of the organisation, as it is the culture that determines how employees conduct their daily tasks (Beach, 1993, p 11). This relationship should represent the situation whereby senior management’s vision for the protection of information in the organisation is conveyed through the Corporate Information Security Policy.

This policy should be drafted, advocated and implemented in such a way that it positively influences the corporate culture with regard to information security. Further, as information security is highly dependent on the behaviour of users, the corporate culture should contribute towards the fact that the de facto behaviour of users is indeed what senior management envisaged as acceptable behaviour. This relationship can be encompassed by the term ‘Information Security Obedience’. Obedience is defined as ‘compliance with that which is required by authority’ (Dictionary.com, 2003, online). The authority in this case is the senior management of organisations, striving towards effective corporate governance. Another definition is, ‘words or actions denoting submission to authority’ (Dictionary.com, 2003, online). As has been said, the words or actions of employees are, to a large extent, determined by the corporate culture in an organisation.
Therefore, by using the term ‘Information Security Obedience’, it binds together all three fields of information security, corporate governance and corporate culture. The term does this by stating that the actions of the employees must comply with that which is required by senior management in terms of information security. Therefore, ‘Information Security Obedience’ is defined, for the purposes of this paper, as ‘de facto user behaviour complying with the vision of senior management as defined in the Corporate Information Security Policy’.

6. CONCLUSION

Information is important to any organisation. However, the protection of this information through information security still forms a very small part in the overall corporate governance strategy. Senior management must be made aware that the protection of information should be its responsibility and management should create the policy necessary to ensure information security in the organisation. One of the problems facing information security is the behaviour of employees.

Most employees do not understand the importance of protecting information, and this lack of understanding is reflected in their negligent information security practices. The Corporate Information Security Policy should describe the vision and goals of senior management in relation to information security. This policy should then be implemented in the organisation in such a way that it affects the behaviour of the users. To ensure the behaviour of employees change favourably towards information security practices, it should become second-nature behaviour in the daily activities. ‘Information Security Obedience’ is the solution to ensuring proper information security behaviour.

This paper defined the term ‘Information Security Obedience’. It explored the relationships between the three fields of information security, corporate governance and corporate culture, and highlighted the importance of binding these fields together. Further research will be conducted to investigate how current information security practices should be modified to have an effect on corporate culture. The manner in which the Corporate Information Security Policy is drafted and implemented in an organisation
will be investigated. A further paper will highlight how ‘Information Security Obedience’ can be used to integrate the three fields and what actions must be taken to do so.

7. REFERENCES


