UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

Cultivating and Assessing Information Security Culture

by

Adéle da Veiga

Thesis

submitted in fulfilment of the requirements for the degree
Doctor of Philosophy

in the subject of
Information Technology

in the
Faculty of Engineering, Built Environment and Information Technology
at the
University of Pretoria

Supervisor
Prof. J.H.P. Eloff

September 2008

Abstract

The manner in which employees perceive and interact (behave) with controls implemented to protect information assets is one of the main threats to the protection of such assets and the effective use of information security controls. Should the interaction not be conducive to the protection of the information assets, it could have a profound impact on the profit of an organisation, productive working hours could be lost, confidential information might be disclosed to unauthorised people and compliance with legal and regulatory regulations could be affected – all this, despite the fact that adequate technical and procedural controls might be in place.

Current research highlights the importance of a strong information security culture to address the threat that employee behaviour poses to the protection of information assets. Various research perspectives propose how an acceptable level of information security culture should be cultivated, and how to assess this culture to determine whether it is on an acceptable level. These approaches are however not adequate to cultivate information security culture, as all the relevant information security components and the influences on the information security culture have to be considered. This leads to the question as to whether the assessment instruments proposed to assess the information security culture are indeed adequate and valid.

The main contribution of this research relates to the development of an information security culture framework and process consisting of an assessment instrument to assess information security culture. In order to develop the information security culture framework, the researcher developed a Comprehensive Information Security Framework (CISF) that equips organisations with a holistic approach to the implementation of information security. The framework provides a single point of reference for the governance of information security.

The Information Security Culture Framework (ISCF) is developed using the CISF as foundation. The ISCF can be used by organisations to cultivate an

information security culture conducive to the protection of information assets. It considers all the components required for information security culture, namely information security, organisational culture and organisational behaviour. It integrates the aforementioned concepts and illustrates the influence between the components.

The ISCF further serves as a basis for designing an information security culture assessment instrument. This instrument is incorporated as part of an Information Security Culture Assessment process (ISCULA) defined by the researcher. ISCULA provides management with the steps to conduct an information security culture assessment, as well as the steps to validate the assessment instrument.

The application of ISCULA is tested in an empirical study conducted in an organisation. It illustrates how to validate an information security culture assessment instrument by ensuring that it is designed based on the ISCF and meets the statistical requirements for a valid and reliable assessment instrument. Both the ISCF and the ISCULA process can ultimately be deployed by organisations to minimise the threat that employee behaviour poses to the protection of information assets.

Summary

Title: Cultivating and assessing information security culture

Candidate: Adéle da Veiga

Supervisor: Prof. J.H.P. Eloff

Department: Department of Computer Science, Faculty of Engineering, Built Environment and Information Technology

Degree: Doctor of Philosophy in Information Technology

Keywords: Information security, information security culture, cultivate, assess, framework, organisational culture, organisational behaviour, questionnaire, process

I dedicate this thesis to my husband, Willem.

Acknowledgements

First of all, I give praise to the Lord who gave me the strength and ability to perform this research study.

Furthermore, I would also like to express my sincere thanks to the following persons for their respective contributions:

– My parents, Nico and Ellen, who provided me with support and motivation throughout my life and instilled qualities in me that enabled me to complete this study;

– My husband, Willem, daughter, Shadonise, and son, Tiago, for their support and understanding during the completion of this thesis;

– My promotor, Professor Jan Eloff, for his motivation, wisdom and excellent guidance, and especially for the manner in which he inspired the best in me;

– Rina Owen, who assisted with the statistical analysis of the survey results;

– Isabel Claassen, for the efficient manner in which she performed the language editing of the thesis;

– the Organisational Diagnostics personnel who assisted with the empirical study and reporting of the results; and

– all the organisations that participated in the research study and thus ensured the success thereof.

PART I

Chapter 1 Introduction

Chapter 2 Defining an Information Security Culture

Chapter 3 Current Research Perspectives

List of Figures

List of Tables

PART I

CHAPTER 1

Introduction

1.1 INTRODUCTION

This research study investigates the information security culture within organisations so as to direct the interaction of humans with computer information systems and contribute to the protection of information assets. The objective is to provide an approach aimed at cultivating an information security culture in an organisation and to assess whether this culture is on an acceptable level. The results obtained from such an assessment can be used to direct human interaction with information assets and thereby minimise the threats that user behaviour poses to the protection of information assets.

Chapter 1 provides some background to and motivation for this research, which leads to the formulation of pertinent research questions. The aims of the research are based on the aforementioned, and are followed by a discussion of the specific terminology. Finally, the manner in which the different chapters will be presented is discussed.

1.2 BACKGROUND TO AND MOTIVATION FOR THE RESEARCH

This research thesis is entitled “Cultivating and Assessing Information Security Culture”. To understand the context of the thesis, background on information security culture in general is provided in this section, focusing on what it is and why it is necessary in the business environment. The discussion is followed by an explanation of what is meant when using the term “cultivating” information security culture and secondly “assessing” that information security culture. A summary of current research work pertaining to the cultivation and assessment of an information security culture follows next, and the section concludes with the motivation for the research questions based on the background provided for cultivating and assessing an information security culture.

1.2.1 What is an information security culture?

A formal definition for an information security culture that applies specifically to this research project will be developed in later chapters. However, for the purpose of this background discussion, the following introductory ideas set the scene for an understanding of the concept of information security culture and the formulation of pertinent research questions.

An information security culture concerns the manner in which employees perceive and interact (behave) with the controls that are implemented to protect computer and information systems and assets in the organisation.

The Information Security Forum (ISF 2000) provides a comprehensive definition for an information security culture. They define it as "the shared values ('what is important') and beliefs (about 'how things work') that people in the organisation have about information security". They argue that it stems from the interaction of employees with the organisation's systems and procedures to influence their behaviour ('the way we do things around here'). Employee behaviour stems from the values and attitudes adopted by employees, as well as from what is required by the organisation's systems and procedures. The behaviour exhibited can result either in the protection of information assets or in incidents compromising the protection of information.

According to Martins and Eloff (2002) an information security culture involves information security characteristics and organisational values (such as integrity). It incorporates the assumption about the type of behaviour that is acceptable and encouraged and that which is not. An example of a behaviour that is encouraged could be to dispose of confidential documents in secure bins.

According to Schlienger and Teufel (2005) an information security culture is ultimately visible in the beliefs, values and artifacts of an organisation. For instance, the employees could believe that they are responsible for the protection of information. As a value the organisation could focus on

innovation and state-of-the-art technology. Information security induction training could be visible as an artifact.

1.2.2 Why is an information security culture necessary?

The risk that employee behaviour poses to the protection of information assets is one of the primary motivations for focusing on cultivating an acceptable information security culture. Another motivation that relates to the first is the heightened regulatory requirements to ensure adequate internal control in an organisation. Both motivations are discussed below.

According to McIlwrath (2006) two to three percent of an organisation's annual profit is potentially lost due to information security incidents. Employees are involved in up to 80% of information security incidents (Walton CB & Walton-Mackenzie Limited 2006). It is clear from these statistics that organisations are potentially losing profit as a result of incidents caused by employees. This view is further supported by a survey conducted by PriceWaterhouseCoopers (PWC 2004) which concluded that "human error rather than technology is the root cause of most security breaches". As such the human element, which poses the greatest information security threat to any organisation, urgently needs to be addressed (Andric 2007, Furnell 2004).

A lack of internal control to mitigate the risk that employees pose to information assets could result in non-compliance with regulatory requirements. According to Bresz (2004), an organisation may be at risk if it does not comply with the Health Insurance Portability and Accountability Act (HIPAA) Security Standard 164.312 (a)(1) (HIPAA 2006) and does not have reasonable and appropriate information security awareness and training programmes in place.

The Sarbanes-Oxley Act (Donaldson 2005) mandates that auditors certify the adequacy of an organisation's internal controls. There is, however, always the potential that human error or circumvention of controls could lead to

misstatements despite the fact that internal controls have been designed effectively (Deloitte & Touche LLP, Ernst & Young LLP, KPMG LLP & PricewaterhouseCoopers LLP 2004). The effectiveness of internal controls designed to protect the integrity, availability and reliability of information and information technology (IT) systems depends on the competency and dependability of the people who are implementing and using them (Kruger & Kearney 2006). The board of directors, having ultimate responsibility for oversight of the financial reporting process (Deloitte & Touche et al. 2004), must ensure that effective controls are implemented to minimise this risk.

One measure that could be considered to reduce the risks posed by inside employees is to focus on a security-aware culture (Van der Merwe & Cantale 2007; Furnell 2007; Ruighaver, Maynard & Chang 2006). To manage their security risks, organisations must have a strong culture of security awareness (information security culture) (Ruighaver & Maynard 2006; Von Solms 2006). This will aid the board of directors to govern the protection of information and to minimise human error or circumvention of controls. Tessem and Skaraas (2005) sustain the notion that an information security culture is vital and must be implemented (cultivated) as part of the general organisational culture. This would not only minimise the threat posed by employees, but also improve the security level and success of the whole organisation (Vroom & Von Solms 2004; Ruighaver, Maynard & Chang. 2006).

1.2.3 Cultivating an information security culture

The Oxford Dictionary (1983, 2005) defines cultivate as to “improve, develop (person, mind, manners)”. When considering the cultivation of an information security culture, the focus is on how to develop such a culture up to an acceptable level in the organisation and so protect its information assets.

An information security culture develops as a result of users’ interaction with information security controls (Grant 2005) such as passwords, access cards or the use of anti-virus software. One way of positively directing the cultivation of an information security culture in an organisation is to implement

information security awareness programs (Drevin, Kruger & Steyn 2006; Zakaria 2006; Grant 2005). Another is to use a set of principles designed to cultivate an information security culture that is conducive to the protection of information assets.

A number of researchers have defined principles, guidelines or checklists (Zakaria & Gani 2003; Kraemer & Carayon 2005; Ruighaver, Maynard & Chang 2006; Detert, Schroeder & Mauriel 2000) for cultivating an information security culture. Their work varies in terms of comprehensiveness. Some propose a concrete list of principles that can be followed, whereas others propose concepts that must be considered to influence culture. The focus of their work also varies in terms of the research fields that information security culture is integrated with. The paragraphs that follow provide a brief overview of the current research relating to the cultivation of an information security culture.

Zakaria & Gani (2003) developed a checklist based on the cultural levels of Schein (1985) to promote an information security culture. Schlienger and Teufel (2005) also related their work to the cultural levels of Schein, but incorporated organisational behaviour and how it can be used to influence the information security culture. Kraemer and Carayon (2005) used the organisational culture dimensions of Guldenmund (2000) to propose principles for cultivating an information security culture. Ruighaver, Maynard and Chang (2006) related the phenomenon of an information security culture to the eight dimensions of culture suggested by Detert, Schroeder and Mauriel (2000). Each of these research projects related information security culture to different cultural approaches (Schein 1985; Guldenmund 2000; Detert et al. 2000; Van Niekerk & Von Solms 2006).

Some researchers did not integrate their approach with organisational culture, but focused on other concepts. Tessem and Skaraas (2005) proposed principles that can be considered to influence an information security culture by integrating it with change management, communication and marketing. Thomson, Von Solms and Louw (2006) proposed the Information Security

Shared Tacit Espoused Values (MISSTEV) model that focuses on concept of employee behaviour and how to influence them to ultimately cultivate an information security culture. Martins and Eloff (2002) focused on organisational or employee behaviour on an organisational, group and individual level aimed at cultivating an information security culture. The Organisation for Economic Co-operations and Development (OECD 2002) published guidelines for cultivating an information security culture, which can be used as guidance for auditors when assessing controls (Baggett 2003). The ISF (2000) followed a different approach whereby they consulted with industry to identify principles that can be considered to enhance an information security culture. Dojkovski, Lichtenstein and Warren (2006); Kuusisto and Ilvonen (2003) and Helokunnas and Kuusisto (2003) focused on small and medium enterprises to establish what should be done to cultivate an information security culture.

From the above literature overview it is clear that various approaches are adopted to influence or cultivate an information security culture. Each approach has a different focus, for example organisational culture, organisational or employee behaviour or even change management. The concern raised is whether these different approaches to cultivate an information security culture are effective. An organisation that aims to cultivate an acceptable level of an information security culture would require a single, all-encompassing (considering all the relevant focus areas from the current research approaches) approach that can be used in organisations from any environment or of any size. It is clear from current research that a comprehensive information security culture framework does not exist yet (see Chapter 3 for a more comprehensive overview of the relevant literature).

1.2.4 Assessing an information security culture

The verb “assess” can be defined as ”to estimate the value or quality of” (Oxford Dictionary 1983, 2005). “Assess” in the context of this study refers to identifying whether the level of information security culture is adequate to provide quality protection to information assets. Determining whether the

information security culture is on an adequate level requires that a value for it be determined. In the current research, this value is determined through a quantitative assessment of the information security culture – thus indicating a specific level of information security culture. An acceptable level of information security culture is defined as the level that provides adequate protection to information assets and so succeeds in minimising the threat to the confidentiality, integrity and availability of the information asset.

Assessing human behaviour and specifically information security behaviour is a mystery to many who are responsible for information security (Vroom & Von Solms 2004). Metrics are available to assess changes in information security awareness, such as the number of reported security incidents or percentage of paper waste being shredded (Tesseman & Skaraas 2005). However, assessing an information security culture is more difficult, as security is part of the organisation's business processes (Tesseman & Skaraas 2005). It is, however, important to assess information security culture in order to identify whether the culture is conducive to the protection of information assets. Should it not be, the assessment results can be used to identify remediation action plans to positively influence the information security culture.

It is important to ensure that the questionnaire or instrument used to assess information security culture is reliable and valid (Straub 1989; Straub 1990; Yang, Cai, Zhou & Zhou 2005; McHaney, Hightower & Pearson 2002). This will help to ensure a powerful survey instrument that will provide results upon which sound management decisions can be based. A valid instrument will contribute to ensuring that consistent results are obtained in the assessment and that the latter is free from measurement error (Chau 1999).

Limited information (Schlienger & Teufel 2005; Martins & Eloff 2002) is available on how to assess an information security culture. The two approaches available are discussed briefly in the next paragraphs.

Schlienger and Teufel (2005) designed a questionnaire to obtain an understanding of the official rules supposed to influence the security

behaviour of employees. The researchers did not focus on the design of an information security culture framework that could serve as the foundation for developing an information security culture questionnaire (assessment instrument). They based their questionnaire on the three levels of organisational behaviour of Robbins (2001), as well as on research work performed by Schein (1985) and subsequently developed information security statements relating to it. They performed substantive research to develop a decision support system for analysing the results automatically and for enabling employees to complete the questionnaire online. Schlienger and Teufel further aim to focus on extending the tool to allow benchmarking (2005).

Martins and Eloff (Martins 2002; Martins & Eloff 2002) developed a theoretical information security culture framework as the base for their information security culture questionnaire and the items to assess an information security culture (Martins 2002; Martins & Eloff 2002). Their framework does not incorporate all the components that Schlienger and Teufel considered – for example, organisational culture levels. Furthermore, Martins and Eloff's information security culture questionnaire still needs to be validated (Martins 2002).

Other researchers like Kuusisto and Ilvonen (2003) did not perform extensive research on the assessment of an information security culture. They did not develop an information security culture questionnaire as such, but used ISO / IEC 17799:2000 (ISO 2000) and BS7799-2:2002 (BS7799 2002) as the base for their assessments.

A study of the available literature has showed that there is no assessment approach that considers a comprehensive information security culture framework. Neither is there an approach that uses the same framework as the basis of the instrument for assessing an information security culture. It is doubtful whether it is effective to use one approach to cultivate an information security culture and a different one to assess it, as the focus of each approach varies.

1.3 PROBLEM STATEMENT

Against this background it is evident that management needs to emphasise the human element when devising an approach aimed at governing information security. User behaviour must be directed to minimise the risk of exposure of information assets. But how does management effectively cultivate an information security culture that is on an acceptable level? As yet, there does not exist an approach that combines an information security culture framework and a related assessment instrument and that management can apply to identify developmental areas and derive action plans whereby to render an information security culture conducive to the protection of information assets.

The brief literature background on an information security culture, as discussed in paragraph 1.2, indicates the following overall research problem:

How can one cultivate and assess an information security culture?

The following research questions are next formulated in terms of the research study:

1.3.1 Research questions

Research question 1: What current research perspectives are available to cultivate an information security culture?

Research question 2: What current perspectives and/or methods are available to make an assessment of an information security culture?

Research question 3: What should an information security culture framework comprise of in order to cultivate information security culture?

Research question 4: How does one conduct an assessment of information security culture?

Research question 5: How does one provide valid and reliable results when assessing information security culture?

1.4 RESEARCH SCOPE

Information security research is conducted in a variety of academic disciplines such as Computer Science, Informatics, Economics, Industrial Psychology, Information Systems, Management Information Systems, Mathematics and Statistics. In addition, the topics in each of these areas pertaining specifically to information security could constitute a vast number. For instance, Siponen and Willison (2007) performed a review of 1 280 information security papers between the period 1990 to 2004. They identified 14 categories of information security topics that could be related to 71.95% of all the papers they had reviewed. These topics varied from a strategic and process nature such as security management planning and risk management, to planning of a legal and technical nature, such as operating system security and cryptography.

This thesis relates to a specific research category that spans across more than one academic discipline in order to achieve the research objectives. The researcher responsible for this study therefore outlines below the scope of this research in terms of academic discipline and research category.

The research category of this study is related to information security and more specifically information security culture. The main academic disciplines that are leveraged of are the following:

- Information technology discipline: Information technology is concerned with the use of the technology of computers in terms of hardware, software and services as well as telecommunications and other devices to “create, store, retrieve, transfer, process and present information” (Finance 2008). The

objective is to "integrate data, equipment, personnel, and problem-solving methods in planning and controlling business activities" (NCSU 2008). Olivier further explains information technology as the study of the application of the computer that could range from technical aspects of computing or even focus on the social impact of computing (Olivier 1997). The subject field is narrowed down to information security culture by focusing on the human element (personnel) and man's interaction with information assets, which further relates to human sciences and culminates in industrial psychology. Information security is regarded as the preservation of the confidentiality, integrity and availability of information (ISO17799 2005).

A number of research categories from an information security perspective are relevant when focusing on the human element in information security, for instance information security awareness (Puhakainen 2006; Kruger & Kearney 2006), inside computer crime (Cardinali 1995) and information security policy obedience (Vroom & Von Solms 2004; Siponen, Pahnila & Mahmood 2007). All are aimed at minimising the threat that user behaviour poses to the protection of information assets. The objective of this research study is, however, specifically related to information security culture in terms of determining the components of such a culture, how to cultivate it and how to assess it. Although the before-mentioned research categories are also relevant, a detailed overview thereof is excluded from the scope of this research and is rather depicted as part of the components in understanding what information security culture is , as well as the interaction between the components.

- Industrial psychology discipline: Industrial psychology is the study of human behaviour at work (Howell 1993: 622). It is used in the context of this research to understand organisational culture and behaviour as well as how to assess these elements in an organisation. The scope of this research study is limited to organisational culture and behaviour and does not extend to for instance culture, climate or employee satisfaction assessments, which also relate to the culture of an organisation. Attitude

and perception concepts are referred to in this study to understand how information security culture develops and how they play a role in assessing it. It is, however, not part of the main focus, which is to understand how to integrate information security, organisational culture and organisational behaviour to ultimately understand what information security culture is.

- Statistical discipline: Statistics refers to an approach in research whereby "many people are studied and information evaluated with mathematical calculations" (Howell 1993: 627). Quantitative research methods have been deployed with great success in the information security discipline (Schlienger & Teufel 2006; Straub, Boudreau & Gefen 2004; Straub 1990; Workman, Bommer & Straub 2008; Siponen, Pahnila & Mahmood 2007; Woon, Tan & Low 2005). To ensure that the appropriate techniques are employed for the empirical research, the author of this study leverages from the statistical academic discipline. Quantitative research methods (in terms of the process to follow to conduct a survey), as well as instrument development and validation techniques are used from a statistical perspective. These methods are also leveraged of in the research listed above, however only those researchers who used these methods to assess information security culture are considered within the scope of the study.

1.5 RESEARCH METHODOLOGY

The research methodology comprises mainly of a literature review, design phase and an empirical study which includes the following:

- Literature study: The literature study provides an overview of the current research perspectives pertaining to the cultivation and assessment of information security culture. The objective is to establish whether there is a research perspective that involves an approach to cultivate information security culture – one that considers information security, organisational culture and organisational behaviour. Furthermore, to determine whether there is a research perspective that considers an information security

culture framework for both the cultivation and assessment of information security culture. The literature study is conducted first in order to aid in motivating the objective of this research study. Furthermore it identifies the contributions and limitations of each research perspective that can be leveraged of for the remainder of this study.

- Framework design: The framework design component of the research methodology focuses on designing a framework for information security culture. A framework for information security culture is required in order to understand what the components of information security culture are and furthermore to use the framework as the base to design an instrument for assessing information security culture. This is accomplished by investigating literature that could aid the researcher in designing such a framework. As such, the Comprehensive Information Security Framework, CISF, is designed and provides organisations with a holistic approach to implement information security. The CISF is used as the foundation for designing the Information Security Culture Framework (ISCF), which in turn can be applied to understand the components of information security culture, as well as the influence of the components on one another.

- Process design: A process is required to apply the ISCF and to understand how to develop an assessment instrument that is based on the framework. The process design phase uses literature and industry input to design a process for assessing information security culture in an organisation. This process is called the Information Security Culture Assessment (ISCULA) process. ISCULA is used to determine whether an acceptable level of information security culture has been cultivated and if not, to deploy corrective action. It provides management with the steps to conduct an information security culture assessment, as well as the steps to design and validate an information security culture assessment instrument.

- Empirical study: The empirical study of this research focuses on the deployment of ISCULA in an organisation. As part of the empirical study, a pilot assessment (survey) is conducted in a South African financial

institution where an initial assessment instrument is developed and validated. The final assessment instrument is improved using literature (theory) as well as industry input. A second assessment is conducted in a South African member firm of an international audit, advisory and tax organisation so as to improve the assessment instrument and validate it by means of statistical techniques. This aids in providing a valid and reliable assessment instrument from a theoretical, industrial as well as statistical perspective. Survey Tracker (2008), a survey design, distributing and statistical analysis tool, as well as Number Cruncher Statistical Software (NCSS) (Hintze 1997) and Statistical Analysis Software (SAS) (2008) were used as the software to conduct the empirical study and validation of the information security culture questionnaire that had been developed.

1.6 TERMINOLOGY USED

In order to avoid any misunderstanding, it is important to correctly interpret the terminology used in this thesis. The researcher now provides a brief definition of what is meant by the terms information security, organisational or employee behaviour, organisational culture and organisational assets.

1.6.1 Information security

According to Dr Paul Dorey, director, digital business security, BP Plc, "information security provides the management processes, technology and assurance to allow business management to ensure business transactions can be trusted; ensure IT services are usable and can appropriately resist and recover from failures due to error, deliberate attacks or disaster; and ensure critical confidential information is withheld from those who should not have access to it" (Cobit Security 2004: 7).

Every organisation uses information as it is an important asset to the business (IS017799 2005: 1). Information is present in many forms, for example in paper and electronic documents; voice recordings and conversations. It is

stored in electronic databases, back ups, archives and hard copy files; transmitted electronically or by post and even as films and SMSs.

As with other business assets, information requires protection to ensure that it is available and confidential and that its integrity is preserved where necessary (ISO17799 2005: 1; Pfleeger 1997: 4-6). Especially with the widespread use of the Internet, electronic handheld devices and wireless technologies introduce more threats to the protection of information (Cobit Security 2004: 5). Threats such as data theft, fraud, fire, viruses, denial-of-service attacks and even social engineering pose serious risks to the protection of information (Pfleeger 1997: 6-11; ISO17799 2005: 1). These threats, together with careless mistakes and employee ignorance in respect of security controls could lead to severe financial, reputational and other damages to an organisation.

Information security is concerned with implementing adequate controls to protect information assets. These controls must be aligned with the organisation's security objectives and should minimise the risks to which the organisation is exposed (ISO17799 2005: 1). Controls cover a wide spectrum of technology such as firewalls, processes such as change management, and human elements such as information security induction training.

1.6.2 Organisational or employee behaviour

According to Kreitner and Kinicki (1995: 13; Robbins 2001: 7), employee or organisational behaviour is an interdisciplinary field dedicated to the better understanding and management of people at work. They also define three basic levels of behaviour in an organisation, namely the individual, group and organisational level (Robbins 2001: 7, 15). Employees will behave according to what is perceived as correct and acceptable and specific organisational behaviour will surface on each level. Such behaviour also encompasses employee attitudes and the way in which they influence actual performance in organisations (Hellriegel, Slocum & Woodman 1998: 4).

1.6.3 Organisational culture

Schein (1985: 9) defines culture as “a pattern of basic assumptions – invented, discovered, or developed by a given group as it learns to cope with its problems of external adaptation and internal integration – that has worked well enough to be considered valid and, therefore, to be taught to new members as the correct way to perceive, think, and feel in relation to those problems”.

1.6.4 Organisational assets

The ISO17799 (2005: 5, 23) defines an asset as anything that adds value to the organisation. This would include information, for example contracts, training material and strategies; software such as system software and utilities; physical assets such as computer equipment; services like communication services and other utilities such as power and lighting; people with their skills and experiences, and lastly, intangible assets such as the image and reputation of the organisation. For the purpose of defining an information security culture, the focus is on information, people and intangible assets.

1.7 LAYOUT OF THESIS

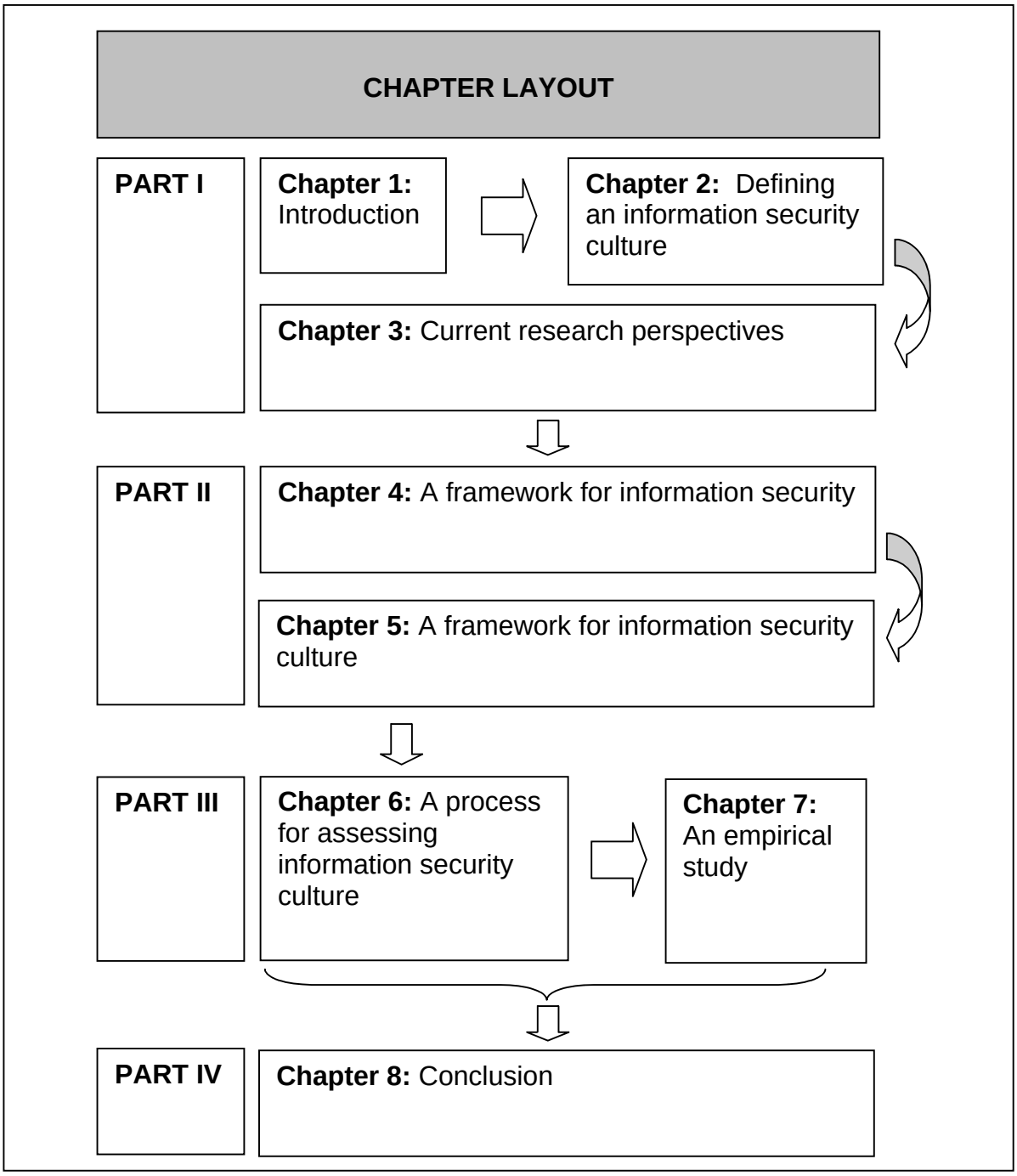
Figure 1.1 provides a graphical depiction of the layout of the thesis and the relationship between the different chapters.

Part I provides some background to the reader and establishes a number of important concepts. The current chapter, **Chapter 1**, explains the rationale behind the study and then proceeds with the formulation of pertinent research questions.

A customised definition for information security culture is presented in **Chapter 2.** This definition serves as reference for the reader to understand

what is meant with the term information security culture when it is used throughout this thesis.

Figure 1.1: Layout of thesis



Chapter 3 evaluates the current research perspectives that focus firstly on how to cultivate and secondly how to assess information security culture in an organisation. The objective is to obtain an understanding of each research

perspective and to identify the contributions and limitations thereof. The outcome aids in providing further motivation for the purpose of this research study.

Part II concentrates on the cultivation of an information security culture in an organisation by understanding what information security culture comprises. **Chapter 4** describes the development of a Comprehensive Information Security Framework (CISF). The author identifies information security components that could influence information security culture in an organisation. These components, in turn, are used to construct a CISF, which serves as the foundation for developing a framework for information security culture.

The Information Security Culture Framework (ISCF) is next developed in **Chapter 5**. This framework is constructed by considering the CISF components, as well as the interaction between organisational culture and organisational behaviour. This interaction is depicted in the framework to illustrate how an information security culture is cultivated.

The focus of **Part III** is on how to assess an information security culture. **Chapter 6** outlines a proposed process, ISCULA, for assessing an information security culture in an organisation. The process also incorporates steps to design and validate an information security culture assessment instrument so as to ensure valid and reliable results.

ISCULA is illustrated and validated in **Chapter 7** by means of an empirical study. The output of the empirical study is a valid and reliable information security culture assessment instrument that can be put to effective use in assessing the information security culture in organisations.

Part IV, Chapter 8, concludes the thesis.

CHAPTER 2

Defining an Information Security Culture

2.1 INTRODUCTION

Chapter 2 aims to formulate a customised and understandable definition of information security culture. This definition will serve as reference to understand what is meant whenever the term information security culture is used throughout this thesis. The definitions of information security culture obtained from current literature are evaluated against key focus areas in order to formulate a customised definition for the purposes of this research.

2.2 DEFINITION OF AN INFORMATION SECURITY CULTURE

Not all of the researchers working in the information security culture field prepared a formal definition of information security culture. Three research perspectives, however, provide definitions for information security culture within the context and scope of this research, namely Martins and Eloff (Martins 2002; Martins & Eloff 2002), Schlienger and Teufel (2002, 2003a, 2003b, 2005) and the Information Security Forum (ISF 2000). As these definitions relate to the scope of information security culture as defined for this research, they will be used as the basis for the formulation of a specific, customised definition of an information security culture to be used in this research.

To formulate such a purpose-made definition, it is necessary to compare the available definitions and identify the similarities and different focus areas of each. Thus, a summary of each of the definitions is provided in the next paragraphs, where after these definitions will be compared against the identified focus areas.

2.2.1 The Information Security Forum

The Information Security Forum (ISF 2000) explains information security culture by relating it to industrial safety in organisations where the safety culture is measured by the number of incidents that occur. They argue that information security incidents in an organisation occur as a result of a series of events that compromise the integrity, availability or confidentiality of information. These events relate to the behaviour of employees or their interaction with information and systems. The behaviour of employees is influenced by their values and beliefs with regard to information security on the one hand and by the organisation's policies on the other hand. As such, the behaviour of employees and the number of incidents that occur in the organisation will portray the information security culture of the organisation. To summarise, the ISF definition focuses on the interaction between employees and the organisation's information assets, resulting in certain behaviour and incidents.

2.2.2 Schlienger and Teufel

The researchers Schlienger and Teufel (2002, 2003a, 2003b) defined information security culture by using the definition of corporate culture as earlier defined by Schein. According to Schein (1985) the core substances of corporate culture are the basic assumptions, attitudes and beliefs of employees, which relate to the nature of people, their behaviour and beliefs. Assumptions are values that become embedded and as such are almost taken for granted. These basic assumptions are non-debatable and non-confrontable (Schein 1985: 18).

Organisational or corporate culture is expressed in collective values, norms and knowledge of organisations. Values relate to the sense that people have of what ought to be. Many values are adopted consciously and guide the actions of employees (Schein 1985: 16-17). Such norms and values affect the behaviour of employees and are expressed in the form of artifacts and

creations. Artifacts are the visible output of a culture, for example the written or spoken language or the way status is demonstrated (Schein 1985: 14-15).

By using this definition, Schlienger and Teufel (2002, 2003a, 2003b) relate information security culture to corporate culture, where employees have certain beliefs about information security, such as that "employees are our security assets". The collective values, norms and knowledge could be illustrated by every employee having to behave in accordance with the organisation's information security requirements. Artifacts and creations could relate to employees annually signing off an information security policy acknowledgement statement. Schlienger and Teufel's definition is the only definition that focuses on artifacts. This aids in making the definition understandable and practical, seeing that it highlights the actual output of an organisation's information security culture.

Although behaviour is not specifically mentioned as part of the definition, the researchers refer to it when assessing the information security culture. Incidents are also not referred to specifically in the definition. They could, however, fall under artifacts as a visible output of the information security culture.

2.2.3 Martins and Eloff

Martins and Eloff (2002) use the definitions of organisation culture and organisational behaviour to define information security culture. They see it as a set of information security characteristics valued by the organisation, such as integrity, confidentiality and availability of information. They also relate it to the assumption about what behaviour is regarded as acceptable in protecting information and what not. The concept of an information security culture further extends to the type of behaviour that is encouraged to protect information and that which is not. The researchers' emphasis is on the behaviour that is present as a result of the attitudes and values of employees, since such behaviour leads to the development of an information security culture.

The definition by Martins and Eloff (2002) does not mention information security incidents, but concentrates on "acceptable" and "unacceptable" behaviour. One could argue that unacceptable behaviour relates to incidents, but this is not mentioned specifically in the definition. The definition also does also not address corporate culture, which Schlienger and Teufel incorporated. One could argue that the assumption about what is acceptable and what is not, could (as stated by Martins and Eloff) relate to the attitudes, assumptions and values defined by Schein. Similarly, the set of characteristics valued by the organisation could relate to the values and knowledge defined by Schein.

2.2.4 Summary of the definitions of information security culture

The three information security culture definitions that are available can be summed up as follows:

- Information Security Forum: Information security culture refers to the shared values ('what is important') and beliefs (about 'how things work') that people in the organisation have about information security. It interacts with the organisation's systems and procedures to influence behaviour ('the way we do things around here') (ISF 2000).
- Schlienger and Teufel: Information security culture has three focus areas namely artifacts and creations; collective values, norms and knowledge; and basic assumptions and beliefs.
- Martins and Eloff: An information security culture emerges from the assumption about what characteristics and behaviour are encouraged to be acceptable, and it results in the manner people behave with regard to information security in the organisation.

From the above synopsis, the following five focus areas pertaining to information security culture are identified:

- Attitudes, assumptions and beliefs (from Schlienger and Teufel and the ISF)
- Values and knowledge (from Schlienger and Teufel and the ISF)
- Artifacts and creations (from Schlienger and Teufel)
- Behaviour (from Martins and Eloff, Schlienger and Teufel)

- Incidents (from the ISF)

The five focus areas are not encapsulated in a single definition. In addition, none of the definitions focus on the concept of time. Ashkanasy, Wilderom and Peterson (2000:117) state that the concept of time is generally ignored by researchers in the organisational science field. They believe that time should be considered when referring to culture as everything in human life revolves around a timeframe. A person's perceptions of an issue can change from year to year as he/she is exposed to situations and gains life experience. In the same manner, employees who have worked for an organisation for a longer period could be more positive about the protection of information assets and perceive it in a different manner, compared to employees who have worked for the organisation for less than a year. For the purpose of this research, study time refers to the development of culture over a period of time and the effect that time has on the perception of employees working in an organisation.

In an attempt to formulate a customised definition of information security culture, the next section compares the current information security culture definitions, identifies areas of overlap and points out the shortfalls in terms of the focus areas identified.

2.3 COMPARING THE DIFFERENT INFORMATION SECURITY CULTURE DEFINITIONS

The key elements of the information security culture definition by each of the researchers are presented in Table 2.1. The objective of Table 2.1 is to determine which one of the three definitions represents the most inclusive or complete definition of information security culture in order to formulate a customised definition. The definitions are matched up to the five focus areas as well as to the concept of "time" identified in Paragraph 2.2.3.

Table 2.1 A comparison of the key elements of an information security culture and the available definitions

Focus areas	Information Security Forum	Martins & Eloff	Schlienger & Teufel
Attitudes, assumptions and beliefs	Shared values ('what is important') that people in the organisation have about information security.	The assumption about what is acceptable and what is not, in relation to information security.	Employees have certain beliefs about information security.
Values and knowledge	Shared beliefs (about 'how things work') that people in the organisation have about information security.	Set of information security characteristics that the organisation values.	Collective values, norms about information security. Knowledge is evident.
Artifacts and creations	-	-	Artifacts and creations are evident.
Behaviour	Employees interact with the organisation's systems and procedures, resulting in a specific behaviour ('the way we do things around here').	The assumption about what behaviour regarding the protection of information is encouraged and what is not. The way people behave towards information security in the organisation.	Behaviour is addressed in the assessment tool of the researchers.
Incidents	Incidents reflect the information security culture of the organisation.	Could be part of the unacceptable behaviour.	Could be part of artifacts.
Time	-	-	-

It is evident from the above table that there is not a single definition that incorporates all the focus areas. The definition by Schlienger and Teufel is the most comprehensive in defining an information security culture (the concept of time excluded) from the definitions listed in Table 2.1. The definition of the ISF

and Martins and Eloff addresses all the focus areas apart from artifacts, creations and time. The ISF definition specifically mentions *incidents,* whereas Martins and Eloff emphasise the *behavioural aspect*. Schlienger and Teufel specifically focus on the output of information security culture in terms of *artifacts, values and assumptions*. Each of these contributions would need to be considered in the definition formulated for this research study. The next paragraph aims to formulate the information security culture definition that will be used for the purposes of this research.

2.4 INFORMATION SECURITY CULTURE AS DEFINED FOR THIS RESEARCH STUDY

By encapsulating the focus areas highlighted in each researcher's definition and adding the concept of time, a customised definition of information security culture is formulated. Such a definition has to serve as a single point of reference to understand what is meant by the term information security culture. The proposed information security culture definition that is provided below will be used for the purposes of this research study.

An information security culture is defined as the attitudes, assumptions, beliefs, values and knowledge that employees/stakeholders use to interact with the organisation's systems and procedures at any point in time. The interaction results in acceptable or unacceptable behaviour (i.e. incidents) evident in artifacts and creations that become part of the way things are done in an organisation to protect its information assets. This information security culture changes over time.

2.5 CONCLUSION

There is a need for a single point of reference to understand what is meant by the term information security culture. Having considered the definitions of the Information Security Forum, Schlienger and Teufel, and Martins and Eloff, the author proposes in Chapter 2 a customised definition of an information

security culture to be used in this study. Two of the original definitions overlap in terms of focusing on organisational culture and behaviour to protect information assets. The Information Security Forum in turn considers the concept of incidents. None of the definitions however consider the concept of time, in other words the development of culture over a period of time.

The newly proposed definition of an information security culture goes beyond encapsulating the current literature definitions and, in addition, considers the concept of time (see Paragraph 2.4). It will be used as reference for the remainder of this research to understand what is meant whenever the term information security culture is used.

Chapter 3 addresses the first and second research questions, and attempts to understand the current information security culture perspectives with regard to cultivating and assessing an information security culture.

CHAPTER 3

Current Research Perspectives

3.1 INTRODUCTION

Chapter 3 discusses the current research perspectives on the cultivation and assessment of information security culture that are available in the literature.. The research perspectives are evaluated against criteria, compiled by the author, to identify the contributions and limitations of each perspective. Herewith the author attempts to establish whether there is a research perspective that comprises of an approach to cultivate information security culture – one that considers information security, organisational culture and organisational behaviour to effectively cultivate a culture conducive to the protection of information assets. Furthermore, she tries to determine whether there is a research perspective that considers a comprehensive information security culture framework for both the cultivation and assessment of information security culture and to effectively minimise the risk that employee behaviour poses to the protection of information assets.

Herewith the first and second research questions are addressed, namely to understand the current research perspectives on cultivating and assessing information security culture. The chapter concludes by highlighting further research that is required, based on the limitations of the current research perspectives.

3.2 CURRENT PERSPECTIVES ON INFORMATION SECURITY CULTURE RESEARCH

A perspective is defined as *the aspect (particular component) of a subject and its parts* (Oxford Dictionary 1983, 2005). Using this definition, the "*subject*" relates to information security culture. The author aims to identify the research conducted in the subject field of information security culture, as well as the different aspects of each research perspective. Therefore, the remainder of

this chapter discusses how the scope of the subject field was determined and aims to identify the research perspectives that fall within this defined scope. An overview of each research perspective is provided in order to identify contributions made to the information security culture subject field, as well as aspects that are lacking.

3.2.1 The scope of current perspectives on information security culture research

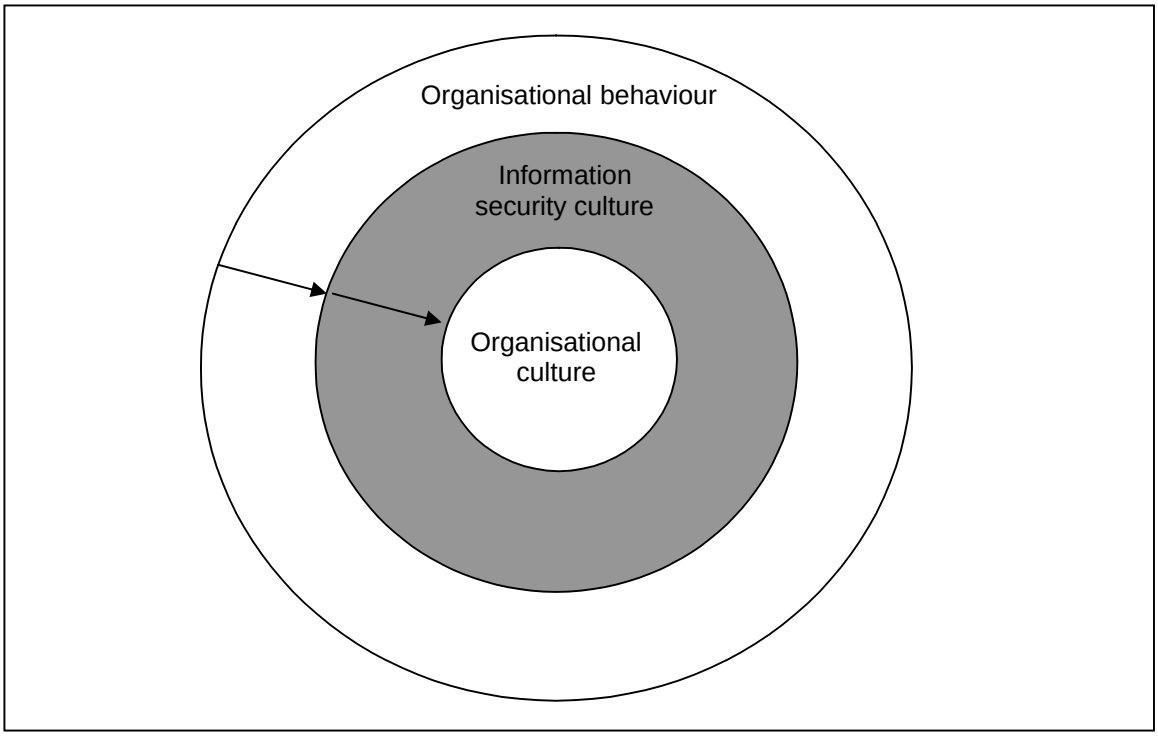
Various researchers have focused on the threat that employee behaviour poses to information assets and how a security-aware culture could contribute to improving the protection of information assets. These perspectives vary in depth of research regarding information security culture. Some researchers only focus on defining information security culture (Nosworthy 2000; Kuusisto & Illoven 2003) or on developing an improved understanding of the concept (OECD 2005; Tessem & Skaraas 2005). Others (Schlienger & Teufel 2005; Martins & Eloff 2002) performed in-depth research to define a way in which to cultivate and assess an information security culture. Some researchers also focus on the behaviour of employees and their interaction with information systems (Thomson & Von Solms 2006; Albrechtsen 2007), but do not concentrate specifically on the information security culture that develops as a result of such behaviour. Furthermore, many researchers (Robbins 2001; Kreitner & Kinicki 1995; Berry & Houston 1993; Schein 1985) investigate the field of organisational behaviour and the way in which an organisational culture develops, in an attempt to understand how to cultivate an information security culture.

To obtain an overview of the current research perspectives aimed at cultivating and assessing information security culture, the author performed a literature review of the researchers involved in this field. The organisational culture and organisational behaviour research fields are not the prime focus of this research study, but were investigated to understand how they influence the concept of information security culture. In order to understand the scope of

current research perspectives, the next section provides a high-level overview of those perspectives that focus on information security culture.

Figure 3.1 depicts the research areas discussed above, namely organisational behaviour (A), information security culture (B) and organisational culture (C).

Figure 3.1 Research areas (layers)



These three research areas have an impact on one another, hence the arrows pointing inwards from the outer to the inner layer. The interaction between the three research areas or layers can be explained as follows:

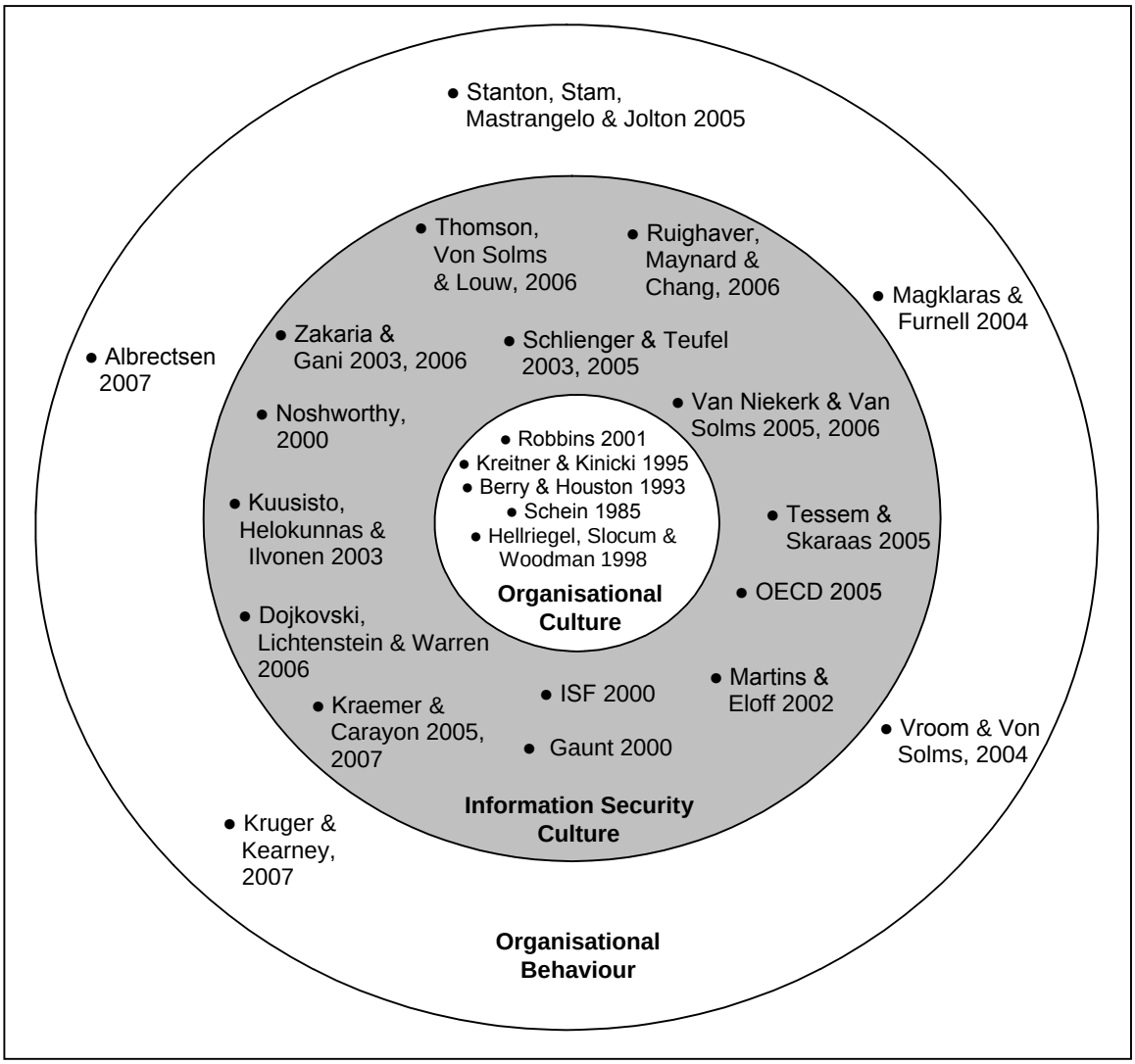
With time, the behaviour exhibited by employees develops to establish a culture embraced by the organisation (Hellriegel, Slocum & Woodman 1998; Robbins 2001). Thus, the behaviour that employees exhibit when interacting with the computer and information systems (CIS) (A) evolves into the information security culture (B) of the organisation. The outer layer focuses on employee behaviour and how this could relate to vulnerabilities in the CIS (Albrectsen 2007; Kruger & Kearney 2007; Magklaras & Furnell 2004, Stanton, Stam, Mastrangelo & Jolton 2005; Vroom & Von Solms 2004). It is

this behaviour (A) that in time establishes the information security culture (B) that forms part of the overall organisational culture (C).

Organisational culture is depicted in the middle layer of the figure. It plays an important role in the implementation of information security (Andress 2000; Connolly 2000; Nosworthy 2000) and may even hinder such implementation if changes are required (Nosworthy 2000). Le Grand and Ozier (2000) argue that good information security practices, e.g. policies and making backups, are not instilled in an organisation through regulation, incentives or monitoring, but they must be embedded in the organisation's culture.

Figure 3.2 expands on Figure 3.1 and portrays the research perspectives in the information security culture layer since this is the prime subject field that is being investigated. Limited research perspectives in the organisational culture and organisational behaviour subject fields are depicted in the diagram to explain the context of these areas. The research perspectives on organisational culture and organisational behaviour are listed for illustration purposes, as only a limited investigation was conducted in this subject field to understand how it relates to information security culture. A discussion is therefore not provided for layers C and A. The research conducted in those research disciplines is used in later chapters as part of the framework development and to understand how information security culture develops. The objective of discussing the research perspectives in the information security culture layer (B) is to understand what research has been conducted in this subject area and to identify the contributions and limitations of each to comply with the objective of this research study.

Figure 3.2 Current research perspectives on information security culture



3.2.2 Current perspectives on information security culture research – contributions and limitations

Various research studies have been conducted in the information security culture field about the definition (Martins & Eloff 2002; ISF 2000), principles (Zakaria & Gani 2003; OECD 2005) and frameworks (Dojkovski, Lichtenstein & Warren 2006) that could be used to cultivate information security culture. Studies were also done on the assessment (Martins & Eloff 2002; Schlienger & Teufel 2005) of an information security culture.

Table 3.1 lists the researchers in the information security culture research layer that was depicted in Figure 3.2. The table provides a summary of the

each of the current research perspectives on information security culture. In the first column the various researchers are listed in chronological order according to the year in which their research work was published. The second column indicates whether or not the research perspective offered by this particular researcher provided a definition for information security culture. This is important to understand the context of the research performed by each of the researchers, as well as to understand whether the research applies to information security culture as defined in this research study.

The remainder of the table is divided into two distinct sections, namely to indicate whether information security culture is cultivated and assessed in terms of the perspective concerned. Various criteria relating to the concepts "cultivate" and "assess", being the scope of this research, are used to determine which author/s give/s the most comprehensive perspective with regard to the defined criteria. A comprehensive information security culture perspective is considered one that defines information security culture, uses an approach to cultivate an information security culture, considers how employee behaviour and culture are influenced in the organisation, as well as considers a reliable assessment instrument to assess information security culture.

The criteria used in Table 3.1 are derived by considering the following:

- The definition for information security culture in Chapter 2 is referred to and as such the criteria "organisational behaviour tiers" and "culture levels" are defined.
- The researcher conducting this study selected the survey method for assessing information security culture. Hence the criteria pertaining to "assess", namely "questionnaire", "content validity", "construct validity" and "reliability" are used as these are required for a valid assessment instrument (questionnaire).
- A framework is required to develop a valid assessment instrument – thus the "framework" criteria. As some researchers did not develop a framework for information security culture, but mention the principles that can be used to develop a framework, the "principles" criteria are used.

A description of each of the criteria is provided in the text that follows Table 3.1. An inclusion tick (✓) is used to indicate whether a research perspective addresses the specific criteria listed.

Table 3.1 Research perspectives on an information security culture

Research perspective		Definition	Cultivate				Assess				Total number of ticks
			Principles	Framework	Organisational behaviour tiers	Culture levels	Assessment instrument (Questionnaire)	Assessment instrument			
								Content validity	Construct validity	Reliability	
1	Gaunt (2000)	-	-	-	-	-	-	-	-	-	0
2	Nosworthy (2000)	✓	✓	-	-	-	-	-	-	-	2
3	Information Security Forum (2000)	✓	✓	-	-	-	-	-	-	-	2
4	Martins and Eloff (2002)	✓	✓	✓	✓	-	✓	✓	-	-	6
5	Kuusisto, Ilvonen, Helokunnas and Kuusisto (2003)	✓	✓	-	-	-	✓	-	-	-	3
6	Zakaria and Gani (2003, 2006)	-	✓	-	-	✓	-	-	-	-	2

Research perspective		Definition	Cultivate				Assess				Total number of ticks
			Principles	Framework	Organisational behaviour tiers	Culture levels	Assessment instrument (Questionnaire)	Assessment instrument			
								Content validity	Construct validity	Reliability	
7	Schlienger and Teufel (2002, 2003, 2005)	✓	✓	-	✓	✓	✓	✓	✓	✓	8
8	OECD (2005)	-	✓	-	-	-	-	-	-	-	1
9	Tessem and Skaraas (2005)	-	✓	-	-	-	-	-	-	-	1
10	Dojkovski, Lichtenstein and Warren (2006)	-	✓	✓	-	-	-	-	-	-	2
11	Thomson, Von Solms and Louw (2006)	-	✓	-	-	✓	-	-	-	-	2
12	Kraemer and Carayon (2005, 2007)	-	✓	-	-	✓	-	-	-	-	2

Research perspective		Definition	Cultivate				Assess				Total number of ticks
			Principles	Framework	Organisational behaviour tiers	Culture levels	Assessment instrument (Questionnaire)	Assessment instrument			
								Content validity	Construct validity	Reliability	
13	Ruighaver, Maynard and Chang (2006)	-	✓	✓	-	✓	-	-	-	-	3
14	Van Niekerk and Von Solms (2005, 2006)	✓	✓	✓	-	✓	-	-	-	-	4

In the first section, four criteria are used to evaluate the research perspectives under the heading “cultivate”. These criteria are the following:

- Principles: Principles refer to the fundamentals of information security culture (Oxford Dictionary 1983, 2005), in other words what is required or should be considered when cultivating an information security culture. Compiling and implementing an information security policy is an example of such a principle.
- Framework: The Oxford Dictionary (1983, 2005) defines a framework as a structure upon or into which contents can be put and further relates it to thoughts that are directed for a purpose. Therefore framework refers to an information security culture framework that can be used to direct or, as such, cultivate an information security culture in an organisation. The framework presents the different components of information security culture and illustrates the interaction and influence between these components. Management has to implement this culture effectively and therefore needs to decide which components (e.g. risk assessment and training) to implement first, as well as on what level to implement them in the organisation (e.g. organisational, group or individual level) (Robbins 2001).
- Organisational behaviour tiers: This criterion relates to the three organisational behaviour tiers defined by Robbins, Odendaal and Roodt (2003: 15) – the organisational (formal structures in the organisation e.g. hierarchical or flat structure); group (employees as members of a group in an organisation) and individual (individuals with their characteristics e.g. age). All three these behaviour tiers develop towards the information security culture of the organisation.
- Culture levels: Schein (1985: 13-21) defined three levels of organisational culture, namely artifacts (visible output such as technology), values (beliefs of the individual) and assumptions (unconscious ideas).

The second section of Table 3.1 relates to “assessing” an information security culture. A survey approach employing a questionnaire (assessment instrument) can be used as the method to assess information security

behavioural content in general, and attitude and opinions in particular (Berry & Houston 1993: 61). As such, a questionnaire can be used to study information security culture and the attitude and perception of employees with regard to it. A valid and reliable assessment instrument (questionnaire) must be used to ensure accurate, reliable and stable results that also prove to be valid (Dillon, Madden & Furtle 1993: 294). The criteria that are used to evaluate the research perspectives in terms of "assess" are:

- Assessment instrument (questionnaire): Did the researcher's assessment approach consist of an assessment instrument (questionnaire) approach?
- Content validity: Content validity evaluates the theoretical perspective(s) that drive the measuring instrument and the way in which the theory has been used to develop the items that are assessed for information security culture (Brewerton & Millward 2002: 90; Furnham & Gunter 1993: 45). This means that one needs to first define theoretically what constitutes the cultivation of an information security culture. The theory can then be used as the foundation for developing the questions of the information security culture assessment instrument. An information security culture framework that illustrates the different theoretical components of information security culture and the interaction between the components can be used as the theoretical input to develop an information security culture assessment instrument. It is important to understand that the theory used to develop the assessment instrument must be specific in terms of cultivating an information security culture to ensure that the assessment instrument assesses what it sets out to assess – thereby providing valid results. If questions are included regarding client satisfaction in the sales process, the results will skew the data as they do not directly relate to information security culture. A question regarding effective information security policy training will, however, aid in providing valid data to obtain an indication of the information security culture in the organisation.
- Construct validity: Construct validity is used to assess the robustness of the assessment instrument dimensions (groups of questions or statements) once the theoretical assessment instrument has been compiled (Brewerton & Millward 2002: 92-93). This technique contributes further towards ensuring that valid results are obtained when using the

assessment instrument to conduct an assessment. Questions or statements that are found not to be acceptable in the analysis can be disregarded and questions that relate to each other can be grouped together to improve the interpretation of the results.

- Reliability: Reliability is concerned with the internal consistency of a proposed or existing scale containing a number of questions (Brewerton & Millward 2002: 89, Huysamen 1988: 20). In other words, the information security culture assessment instrument must use questions or statements that assess information security culture accurately and that respondents will interpret in the same manner irrespective of when, where and how the assessment is conducted (Huysamen 1988: 20). If the researchers have indeed performed a statistical analysis of the data of an information security culture assessment to determine the reliability of the assessment instrument, an inclusion tick is provided.

The last column of Table 3.1 shows the total number of ticks, in other words the number of different criteria that each research perspective addresses.

In the paragraphs that follow below, a summary is provided of the perspective offered by each of the researchers/research teams listed in Table 3.1.

3.2.3 Gaunt

The research perspective of Gaunt (2000) concentrates on creating an information security culture within the medical environment. Due to the concerns raised about the protection of patient information, the National Health Service (NHS) in England and Wales and the Chief Medical Officer of England commissioned a review of patient identifiable information. Various recommendations relating to the improvement of the information security culture in the medical environment have emerged from this review. Some involve improved controls for information systems such as access controls and others suggest communication to raise awareness among employees regarding confidential information. Gaunt further suggests that an information security policy would be essential in creating the desired level of information

security culture to protect patient records, but that employees would need to accept the policy.

3.2.3.1 Contributions and limitations of Gaunt's perspective

Gaunt investigates information security culture in a specific industry and aims to understand how it applies to the medical industry. It is important to consider the different industries when cultivating an information security culture. The focus for the financial sector with banking and payment information would differ from that for the mining industry, which will probably have less sensitive information to protect.

Gaunt's research work does not extend to defined principles to cultivate information security, nor to a framework or assessment instrument. He raises awareness regarding the concept on information security culture and states that further work is required to meet the needs of the medical industry and protect patient information.

3.2.4 Nosworthy

Nosworthy's (2000) research relates to the various controls (information security policy, education and training) an organisation should consider when implementing information security. The researcher argues that people and their attitude play a significant role in the success of implementing information security. Should people's attitude change, their behaviour would also change. In essence, if people view information security in a positive manner, they would also behave favourably in terms of complying with information security requirements.

In order to influence people, various information security controls (awareness, training and monitoring) and processes (risk assessment) must be implemented. These controls relate to the "principles' column in Table 3.1, as they highlight what an organisation should consider to change employee behaviour that will in the end contribute to a change in the information security

culture. Nosworthy (2000) argues that the organisational culture could well affect the success of implementing information security and that this fact has to be considered when deploying information security principles.

3.2.4.1 Contributions and limitations of Nosworthy's perspective

Nosworthy's research highlights the importance of considering the organisational culture and how it could influence the implementation of information security controls. She deems it vital not only to consider the organisational culture when cultivating an information security culture, but also to understand how such a culture develops. A key contribution of this research perspective that relates to the current research study is the emphasis placed on the attitude of employees regarding information security and how employees should be guided to change their attitude and behaviour. It also highlights the fact that the attitude of employees at a certain point in time in the past could be different from their attitude in the present. It could be of great value to measure this change in attitude, as one could then obtain an indication of the change that took place and of whether the implemented controls were successful.

Nosworthy does not focus specifically on the concept of information security culture, but rather on information security principles to be implemented. (Such principles could obviously influence the information security culture in an organisation.) Nosworthy does not focus on the assessment of an information security culture either.

3.2.5 Information Security Forum

The Information Security Forum (ISF 2000) defines information security culture by focusing on the interaction between employees and the organisation's information assets, resulting in certain behaviour and incidents (see Chapter 2). Furthermore, the ISF obtained input from focus groups to identify factors that drive people's behaviour with regard to information security. The cultural factors defined by the ISF are management commitment

to information security; organisational norms and priorities about information security; information security capabilities of the organisation; information security rules and procedures; and information risk. Factors identified by the focus groups for the rules and procedures factor are, for example, the perception that information security rules and procedures are important, and adherence to rules and procedures. The factors defined by the ISF relate to the "principle' criterion in Table 3.1, as they contribute towards cultivating an information security culture in an organisation.

3.2.5.1 Contributions and limitations of the ISF's perspective

The approach used by the ISF to define the principles ensures that the principles are practical and address the requirements of industry. A focus group is a good method to ensure usability and effectiveness of a proposed concept. A limitation that could be raised in this instance is that the principles are not based on literature or theory so as to substantiate and afterwards validate them in focus groups.

Currently the ISF's research work does not include an information security culture framework that illustrates the interaction between the principles and how to apply them in an organisation. The principles have also not been used to develop an assessment instrument to assess information security culture. However, the ISF proposes to use the information obtained from the focus groups to develop an assessment instrument for this purpose in future.

3.2.6 Martins and Eloff

Martins and Eloff (Martins 2002; Martins & Eloff 2002) designed an information security culture framework based on the concepts of organisational behaviour (Robbins, Odendaal & Roodt 2003) and what constitutes information security. They identified information security controls that can also be referred to as principles on the individual, group and organisational level of organisational behaviour and that could influence information security culture (Martins 2002; Martins & Eloff 2002), for instance

policy, awareness and change. This theoretical perspective provides the foundation for the information security culture assessment instrument and the items developed by the researchers to assess an information security culture (Martins 2002; Martins & Eloff 2002).

The researchers defined an approach consisting of four phases to conduct an information security culture assessment. They tested the proposed approach in an organisation with a sample consisting of less than 50 employees.

3.2.6.1 Contributions and limitations of Martins and Eloff's perspective

This approach involves a comprehensive definition of information security culture and integrates information security with the knowledge fields of information security and organisational behaviour. The information security culture framework serves as the theoretical base to ensure content validity of the information security culture assessment instrument that has been designed by the researchers, thereby aiding in producing valid results if an assessment was conducted.

The researchers (Martins 2002: 56-66) studied information security controls on the individual, group and organisational level that could influence information security culture and defined nine theoretical components, namely

- information security policy;
- change management;
- risk analysis;
- awareness;
- budget;
- benchmarking;
- ethical conduct; and
- trust.

These components were plotted on the organisational behaviour model of Robbins (Robbins, Odendaal & Roodt 2001: 18) to identify which components

influence information security culture on the organisational, group and individual tier.

A limitation to the approach is that the information security culture framework does not consider organisational culture to understand the output of the framework when implementing it in an organisation (e.g. how the culture will be visible in artifacts and how employee attitudes could be influenced).

Lastly, the information security culture assessment instrument designed by the researchers has not been statistically tested for validity and reliability. Although the assessment instrument is based on theory, its practicality is questionable as it has not been discussed with industry through for instance focus groups.

3.2.7 Kuusisto, Helokunnas and Ilvonen

Kuusisto and Ilvonen (2003) and Helokunnas and Kuusisto (2003) studied the concept of information security culture by focusing on hub organisations that form part of a value net. The concept of a hub organisation relates to an organisation that has information about information sources that are disseminated, collected and shared through its relationships.

The researchers define information security culture as a result of a framework and content. They argue that an information security culture is established by formalising a framework (standardisation, certification and measurement) of information security, as well influencing people's attitude, motivation and knowledge.

Kuusisto and Ilvonen (2003) used ISO/IEC 17799:2000 (ISO 2000) and BS7799-2:2002 (BS7799 2002) standards to perform assessments in small and medium enterprises in Finland to determine the state of information system security. Their assessment focused on the information security

framework and not on the content component (user's attitude, motivation and knowledge) of information security.

Helokunnas and Kuusisto (2003) have further argued that an information security culture is established in organisations through "time-divergent communication" and by promoting knowledge of information security among employees. Time-divergent communications relate to the communication of information security activities conducted in the past, present and future. The communication initiatives address the human aspect and assist in transferring knowledge about the state of information security to employees. Future research by Helokunnas and Kuusisto inted to involve the collection of empirical data to further research time-divergent communication that relates to the content component of information security culture. This will be useful as the focus will be on the human component and how to assess information security culture from this perspective.

3.2.7.1 Contributions and limitations of Kuusisto, Helokunnas and Ilvonen's perspectives

This research work proposes two angles to information security culture, namely framework and content components. It illustrates that information security culture is dependent not only on employee behaviour, but also on organisational processes that could for instance include technology components. This is important as one cannot concentrate only on the employee to understand the information security culture in the organisation and never consider the organisational processes and communication that influence such employee behaviour. The framework and content components could relate to the "principle" criterion of Table 3.1, as the researchers propose that it could aid in cultivating an information security culture in an organisation. The concept of time-divergent communication is equally important, as it will change the way in which employees perceive information security over a period of time and assist in cultivating the required level of information security culture. The researchers did unfortunately not develop a

framework to illustrate the interaction between the framework components and content components that they had defined.

As mentioned earlier, Ilvonen and Kuusisto based their questions in the SME assessments on the ISO/IEC 17799:2000 (ISO 2000) and BS7799-2:2002 (BS 7799 2002) standards. Since these standards are comprehensive, they helped the researchers to obtain an indication of the framework component of their approach. However, they did not focus specifically on culture and change in behaviour, but rather on the controls to be considered in implementing information security in an organisation. Thus the researchers did not assess the content components of their approach, which poses a limitation to their work. Content should be assessed if the information security culture in the organisation is to be understood.

A further limitation to their research involves the fact that the study was developed for small and medium enterprises, which might imply that it is not scalable to larger organisations like banks or insurance organisations that operate on a global basis.

3.2.8 Zakaria and Gani

Zakaria and Gani (2003) proposes a conceptual information security culture checklist. They refer to the checklist as conceptual, as it is not exhaustive in terms of information security. Information security is a dynamic field and new ideas will always emerge; hence the checklist will constantly have to be updated and adapted. The objective of the conceptual checklist is to guide managers in implementing an information security culture, while it also raises awareness among employees about the securing of information.

The checklist is based on the three cultural levels of Schein (1985) and are named as follows: surface manifestation (based on the artifact and creation level of Schein); values (based on the value level of Schein); and basic assumption level (based on the basic assumption level of Schein). Within each of these three levels various checks are defined (e.g. on the surface

manifestation level – artifacts, courses, heroes and language). A factor of interest in information security is next defined for each check. For example, visual personnel security (a staff uniform) may be a factor of interest for an artifact, while general naming (the type of backups performed) may be a factor of interest for language. In total, twenty-six information security factors of interest are defined.

In further research, Zakaria (2006) proposes that concepts of basic information security knowledge can be used to cultivate a culture of information security. He identifies the following five concepts for consideration:

- Basic information security knowledge should cover fundamental aspects – from evaluating current security processes to reviewing incident response procedures.
- All employees should participate in information security knowledge sharing sessions.
- Good peer relationships can promote information security knowledge sharing.
- Basic information security knowledge should include recognition of what is reward and punishment in terms of information security matters.
- All basic information security knowledge should be documented.

3.2.8.1 Contributions and limitations of Zakaria and Gani's perspective

Zakaria and Gani's research illustrates an integration between organisational culture and information security, which serves to enhance information security in an organisation. The organisational culture levels of Schein were effectively used to produce a checklist for information security culture. The checklist provides a good base for understanding what exactly has to be considered when cultivating an information security culture. However, it does not incorporate organisational behaviour, namely to understand how the behaviour of employees is influenced and what levels of behaviour (organisational, group or individual) are influenced. It also does not extend to a standardised assessment instrument that can be used to assess information security culture statistically, but merely suggests a list of factors of interest

that the organisation can check for. As the checklist assists in cultivating an information security culture, it conforms to the criterion of "principle" in Table 3.1

The information security knowledge concepts proposed by Zakaria focus on employees' knowledge about information security that can be used as input for training or awareness initiatives. It does unfortunately not extend to assessing the knowledge levels or the information security culture level in the organisation.

3.2.9 Schlienger and Teufel

The research by Schlienger and Teufel (2002) introduces a paradigm shift – from a technical to a socio-cultural approach towards information security. They conclude that one has to focus on the organisation's culture and address the human element to minimise risk to information assets.

Schlienger and Teufel (2003; 2005) selected the survey method with a assessment instrument together with interviews as means to obtain an understanding of the official rules that are supposed to influence the security behaviour of employees. Their assessment instrument (Schlienger & Teufel 2005) takes into account the three levels of organisational behaviour of Robbins (2001), as well as research work performed by Schein (1985). It includes twelve areas that are measured (leadership, problem management, communication, attitude, etc.) The researchers conducted substantive research and developed a decision support system that not only enables employees to complete the assessment instrument online, but also analyses the results automatically. This assessment tool was implemented in a private bank and its usefulness was clearly illustrated by its application. The Working Group "Information Security Culture" of the FGSec (Information Security Society of Switzerland) also participated through discussions to ensure the practicability of the process and the data was used to validate the assessment instrument (Schlienger 2006).

They have also proposed a cyclical approach for managing and assessing an information security culture. This cyclical approach consist of various phases to assist an organisation in conducting an information security culture assessment.

3.2.9.1 Contributions and limitations of Schlienger and Teufel's perspective

Schlienger and Teufel's research work integrate three research fields – information security, organisational behaviour and organisational culture. They effectively use this integration to understand what information security culture is, as well as to know what is required for cultivating such a culture in an organisation. Their research work does not extend to an information security culture framework that illustrates the interaction and influence between the different components (i.e. organisational behaviour, organisational culture and information security) in the framework and that can be used to cultivate and assess information security culture. Their research has contributed towards the effective development of an assessment instrument that can be used by industry and that has been tested for reliability and validity (Schlienger 2006).

3.2.10 The Organisation for Economic Co-operation and Development (OECD)

In 2002 the Organisation for Economic Co-operation and Development (OECD) published guidelines regarding the security of information systems and networks, and suggested the need to develop a culture of security. According to Baggett (2003), these OECD guidelines would also assist auditors in assessing the control environment of an organisation.

The OECD proposed nine guidelines to promote a culture of security among their participants and to raise awareness about the risk to information assets in the organisation. (Thus, it addresses the "principle" criterion as identified in Table 3.1.) The nine guidelines that were proposed are listed below:

- Awareness: Participants should be aware of the need for security of information systems and networks and they should know what they can do to enhance it.
- Responsibility: All participants are responsible for the security of information systems and networks in the organisation.
- Response: Participants should act in a timely and co-operative manner to prevent, detect and respond to information security incidents.
- Ethics: Participants should respect the legitimate interests of others.
- Democracy: The security of information systems and networks should be compatible with the essential values of a democratic society.
- Risk assessment: Participants should conduct risk assessments.
- Security design and implementation: Participants should incorporate security as an essential element of information systems and networks.
- Security management: Participants should adopt a comprehensive approach towards information security management.
- Reassessment: Participants should review and reassess the security of information systems and networks, and make appropriate modifications to security policies, practices, measures and procedures.

3.2.10.1 Contribution and limitations of the OECD's perspective

The OECD's emphasis on the importance of information security culture assists management in promoting the concept in the organisation. Unfortunately it does not give further details as to how each principle could be implemented. The OECD's guidelines also do not extend to a framework that indicates the interaction between the principles or how to assess them in an organisation.

3.2.11 Tessem and Skaraas

Tessem and Skaraas (2005) draw comparisons between different fields of knowledge to understand how to cultivate an information security culture. They consider information security as part of the organisational culture that has to be integrated with change management, communication and

marketing. Furthermore, they focus on the role that management plays in creating a culture based on the work of Schein (1985). Tessem and Skaraas highlight various principles that an organisation should consider when cultivating an information security culture, thereby meeting the "principle" criterion listed in Table 3.1. The principles defined by the researchers are listed below.

- Long-term plan: The organisation must implement a long-term plan for information security.
- Change management: People resist change and therefore change management must be considered when information security procedures are implemented.
- Management: Management must commit itself to information security and should understand its role.
- Participation: Employees must participate in the information security initiatives of their organisation to ensure ownership and commitment.
- Branding: Marketing initiatives should focus on educating employees about information security. Information security could be branded in the organisation to emphasise the importance thereof and focus employee attention on it.

According to Tessem and Skaraas (2005), organisations should also consider measuring the state/level of their in-house information security culture. They admit that it is difficult to provide empirical data on information security as it does not have a purpose in itself, but supports business processes to add value. They also agree that it is difficult to make an accurate analysis of information security awareness. Some metrics that could nevertheless be considered are the percentage of employees who have completed awareness training; the number of reported information security incidents; the percentage of paper waste shredded; the percentage of weak passwords and customer satisfaction.

3.2.11.1 Contribution and limitations of Tessem and Skaraas's perspective

The research by Tessem and Skaraas (2005) emphasises the need to integrate information security with organisational culture, marketing and communications in order to drive awareness messages to users. Their research however, does not integrate information security with organisational culture or with organisational behaviour to understand how it develops and how it can be influenced. Neither does their work extend to an information security culture framework that explains how the principles influence one another or behaviour to cultivate an information security culture. Although they mention the assessment of information security culture, they do not propose a process that can be used for this purpose. A further limitation of the study by Tessem and Skaraas is that the proposed metrics would unfortunately remain insufficient to assess the overall effect of awareness and level of information security culture.

3.2.12 Dojkovski, Lichtenstein and Warren

Dojkovski, Lichtenstein and Warren (2006) conducted research in Australia aimed at developing a framework that can be used to cultivate an information security culture. They suggest a four-phased approach to design a framework for establishing information security culture in small and medium enterprises (SMEs). Their framework meets the criteria of Table 3.1, as it illustrates the different components an organisation needs to consider, as well as the interaction between the components.

During the first phase of their approach the researchers designed a framework based on a literature review. As part of the second phase, a focus group study was conducted to enhance the framework. Questions were also designed to be used in the third phase to confirm the framework. The third phase involved a case study that was conducted in an engineering SME and in two IT service provider SMEs. The researchers asked the SME employees questions

relating to management and behaviour, electronic learning, individual and organisational learning, and ethical, national and organisational culture.

Three external influences to the framework that could affect the information security culture in an organisation were identified by Dojkovski, Lichtenstein and Warren:

- National and ethical culture: The national culture of a country could influence the information security culture of its organisations. Since the national culture and ethical standards of nations and even organisations differ, different nations and organisations must aim to work together in order to promote a positive information security culture.
- Government initiatives: Governments could assist in cultivating an information security culture in SMEs by various means, such as by disseminating awareness brochures and drafting sample security risk scenarios. Expanding on the research of Martins and Eloff (2002), Dojkovski, Lichtenstein and Warren also suggest that government can play a role in providing information security benchmarking information in the SME environment.
- Vendors: Vendors can help to establish a culture of information security awareness as well as trustworthiness in SMEs, as they supply and sometimes maintain these enterprises' hardware and software.

Various organisational influences and initiatives also play a role in cultivating an information security culture. These influences, together with the external influences and output of the framework, can be seen as the principles of Table 3.1 as they assist in cultivating an information security culture. The particular organisational influences are listed below:

- Leadership and governance: Management of SMEs must illustrate leadership in managing information security and model the behaviour expected of employees.
- Organisational culture: The culture in an organisation will influence its information security culture and should be considered so as to identify the effect it could have on information security.

- Managerial aspects: Various managerial aspects need to be considered. Dojkovski, Lichtenstein and Warren relate these aspects to the controls identified by Martins and Eloff (2002), namely policies and procedures, risk analysis, budget considerations, incident management procedures and resource management through a staff handbook.
- Individual and organisational learning: Various learning methods such as e-learning, training and education should be deployed to further cultivate an information security culture.
- Organisational security awareness: The organisation must implement actions to raise staff awareness of information security. Brown bag sessions or posters are examples of activities that can be considered.
- Continuous review: The information security procedures and measures implemented by organisations should be evaluated on a continuous basis to ensure constant improvement.
- Behaviour: Internal and external initiatives must be deployed to establish desirable behaviour in terms of responsibility, integrity, trust and ethicality.

3.2.12.1 Contributions and limitations of Dojkovski, Lichtenstein and Warren's perspectives

A definite contribution by these researchers has been to highlight the fact that there are various principles (referred to as influences by the researchers) that must be considered to cultivate information security culture and that the principles influence one another as well as the information security culture that is evident in the organisation.

The researchers' framework can be implemented by SMEs in the Australian environment as it was applied as part of the research study. The framework as such has been constructed for the SME environment and not specifically for larger organisations in other areas of the world. It may therefore not be scalable or applicable to other organisations. The framework is constructed mainly by considering input from focus groups, which makes it practical and relevant to the industry. However, existing research regarding information security culture (in terms of organisational culture and behaviour) is not

considered in this approach, which raises concern about the comprehensiveness of the framework. Moreover, Dojkovski, Lichtenstein and Warren's work does not focus on defining information security culture as such, or on proposing a process or assessment instrument to assess the level of information security culture in an organisation.

3.2.13 Thomson, Von Solms and Louw

In 2003 Von Solms R. and Von Solms B. suggested that an information security culture be cultivated through an information security policy. They considered the work of Schein (1985) on organisational culture and argued that employee behaviour can be influenced if the organisation's information security policies are aligned with the organisational culture. They further argued that communication and education are key to manifest the policy requirements in employee behaviour.

In 2006 Thomson, Von Solms and Louw proposed the Information Security Shared Tacit Espoused Values (MISSTEV) model. The aim of this model is to create information security obedience that could lead to the cultivation of an information security culture. Information security obedience is defined by the researchers as behaviour that is in line with the requirements of the organisation's information security policy (Thomson & Von Solms 2005).

The MISSTEV model describes the process and stages of acquiring a new skill or behaviour. The researchers apply it to acquiring a culture of information security and conclude that people will naturally progress through the learning phases. The model further focuses on knowledge creation processes regarding tacit and explicit knowledge to ultimately create knowledge of information security among employees. It also considers the effect on the culture of the organisation as defined by Schein. They argue that the information security policy is the cornerstone for creating information security obedience. As such MISSTEV details the progression from the development of the information security policy to information security obedience, but does not specifically concentrate on the details of cultivating

an information security culture. MISSTEV can relate to the "principle" criterion in Table 3.1, as it can contribute towards cultivating an information security culture.

3.2.13.1 Contributions and limitations of Thomson, Von Solms and Louw's perspective

The work done by these researchers focuses on an approach to create information security knowledge and to cultivate an information security culture over time. Time is an important concept to be considered, as an information security culture can be positively influenced over a period of time. Knowledge of employees is also an important concept that should be taken into account when cultivating or assessing an information security culture. Therefore the focus should not be only on the attitudes and perceptions of employees.

The research work does not specifically integrate the concepts of organisational culture and behaviour to understand how they influence employees' learning and compliance with policies. It does not provide a framework for information security culture either, but rather focuses on learning levels of knowledge. To summarise, the research concerned does not extend to a process or an assessment instrument for assessing information security culture.

3.2.14 Kraemer and Carayon

Kraemer and Carayon (2005, 2007) conducted a study to identify how information security culture relates to the six organisational culture dimensions of Guldenmund (2000). The term "dimension" as used by Kraemer and Carayon also refers to "principles" as defined by the author of the current research study; hence the term principles will be used further on. The six principles of organisational culture defined by Guldenmund are employee participation; training, hiring practices, reward system; management commitment; communications and feedback. A qualitative research approach was used to interview computer and information security managers from

different organisations. The objective was to further define the organisational culture principles. As a result, a preliminary list of comments for each of the six principles was defined.

3.2.14.1 Contributions and limitations of Kraemer and Carayon's perspective

These two researchers have been the first to relate information security culture to the culture dimensions of Guldenmund. It has not yet been established whether their approach is effective and practical in cultivating an information security culture, as it has not yet been deployed or tested in an organisation. Unfortunately their research work does not go as far as a process for assessing information security culture.

3.2.15 Ruighaver, Maynard and Chang

Ruighaver, Maynard and Chang (2006) relate information security culture to the eight dimensions of culture from Detert, Schroeder and Mauriel (2000). (As indicated above, the term "dimensions" is replaced by "principles" in this research study.) The eight principles are the basis of truth and rationality; the nature of time and time horizon; motivation; stability versus change/innovation/personal growth; orientation to work, task, co-workers; isolation versus collaboration/ corporation; control, coordination and responsibility; and orientation and focus – internal and/or external. Ruighaver, Maynard and Chang related information security to these principles, based on a number of case studies performed at organisations.

3.2.15.1 Contributions and limitations of Ruighaver, Maynard and Chang's perspective

The case studies conducted by the above research team to relate information security to culture helps to ensure the practicality of the research perspective. Unfortunately this perspective has not yet been deployed in an organisation to establish whether it is effective in cultivating an information security culture.

Information security culture, integrated with the eight culture principles mentioned, is not formulated into an information security culture framework that would aid in implementing such a culture in an organisation. The research by Ruighaver, Maynard and Chang does not include a process or assessment instrument to assess the information security culture.

3.2.16 Van Niekerk and Von Solms

Van Niekerk and Von Solms (2005) defined an outcomes-based framework for culture change. The framework considers outcomes-based education, organisational learning and corporate culture to address the knowledge and attitude of employees with regard to information security. The reasoning behind this framework is that employees with adequate knowledge but a wrong attitude towards information security will not interact with information assets in a secure manner. Similarly, employees with an acceptable attitude but lacking in knowledge will not be equipped to interact with information assets in the expected manner. Such employees need to be educated. The researchers selected outcomes-based education as a means to address knowledge and attitude in a holistic manner so as to positively influence the information security culture in an organisation.

Van Niekerk and Von Solms (2006) used the organisational culture levels of Schein to compile a framework to better understand information security culture. The original framework consists of three organisational culture levels, namely artifacts, values and assumptions, while Van Niekerk and Von Solms have added knowledge as a fourth level. They relate these four levels to levels of security, where a minimum baseline is used to compare the different culture levels as described below:

- Neutral and Stable: The artifacts, values, assumptions and knowledge levels are on the desired level and do not exceed or fall short of the minimum baseline. The culture is therefore stable and predictable.
- Insecure and Mostly Stable: The values and assumptions meet the required baseline. However, the employees do not have an acceptable

level of information security knowledge to for instance compile an information security policy. Therefore artifacts might not be in place.

- Insecure and Unstable: In this scenario employees lack knowledge and do not have the desired beliefs and values. Assumptions are also below the minimum baseline, resulting in an unstable culture which is not desirable.
- Secure and Unstable: Values and knowledge are adequate. However, employees might not have the desired beliefs and assumptions. This could have the effect that the culture is more secure than the minimum acceptable baseline.

Both the culture change framework and the framework depicting the different culture levels address the "framework" criterion listed in Table 3.1. Knowledge and education can be seen as principles for cultivating an information security culture and are therefore ticked off in the "principle" column of Table 3.1.

3.2.16.1 Contributions and limitations of Van Niekerk and Von Solms's perspective

Change is a valuable contribution to the research perspectives on information security culture. It is important to understand that an information security culture is not passive, but can actively be influenced through education and training. It is also important to recognise that there are various levels of information security culture that could be present in an organisation, and that an organisation can apply education to positively influence the internal level of information security culture.

However, the research perspective held by Van Niekerk and Von Solms does not incorporate organisational behaviour tiers in either framework and does not address the assessment of information security culture.

3.2.17 Summary

Most of the available research perspectives discussed above focus on the principles involved in cultivating an information security culture. Limited

research perspectives focus on cultural levels – six in total (Martins & Eloff 2002; Zakaria & Gani 2006; Thomson, Von Solms & Louw 2006; Kraemer & Carayon 2006; Ruighaver, Maynard & Chang 2006, Van Niekerk & Von Solms 2006) and on organisational behaviour levels – two in total (Martins & Eloff 2002; Schlienger & Teufel 2005). Schlienger and Teufel's approach is the only research work that considers both cultural levels and organisational behaviour levels.

Only four perspectives (Dojkovski, Lichtenstein & Warren 2006; Ruighaver, Maynard & Chang 2006; Martins & Eloff 2002, Van Niekerk & Von Solms 2006) address an information security culture framework. There is, however, no single research perspective that integrates the organisational culture with the organisational behaviour levels to formulate an information security culture framework that illustrates the interaction and influences within the framework. Ideally, the information security culture framework should be used to cultivate an information security culture and to serve as the foundation for the assessment approach. Such a framework will contribute towards identifying all the requirements that an organisation has to consider in cultivating an information security culture. It can serve as a single point of reference and ensure that the approach is comprehensive to cultivate information security culture.

An information security culture framework can further provide direction for formulating an information security culture assessment instrument. This will contribute to the effectiveness of the approach, whereby the same framework can be used for cultivating and assessing an information security culture.

Only three of the above research perspectives (Schlienger & Teufel 2005; Martins & Eloff 2002; Kuusisto and Illvonen 2003) focus on the assessment of an information security culture. In all three cases users have to complete an assessment instrument to obtain an indication of the information security culture in an organisation.

Based on the literature overview that summarises current research perspectives on information security culture, the areas that require further research are listed below.

- An information security culture approach is required to both cultivate and assess information security culture. Such an approach should meet all the criteria in Table 3.1 as defined by the author of this research study.
- An information security culture framework must be defined that illustrates the interaction and influence between information security, organisational culture and organisational behaviour.
- An information security culture assessment instrument that is based on the information security culture framework must be developed to ensure content validity.
- A statistically sound information security culture assessment instrument must be compiled. Statistical analysis should be conducted to confirm the validity and reliability thereof.

3.3 CONCLUSION

Fourteen research perspectives on information security culture were discussed in this chapter. The available research was evaluated in terms of cultivating and assessing an information security culture. Thirteen of the perspectives relate to the cultivation of such a culture and three of them incorporate the assessment of an information security culture. However, none of the perspectives provide an approach that uses the same information security culture framework (considering organisational behaviour and organisational culture) to assess and cultivate an information security culture. Moreover, none of the perspectives provide a statistically sound assessment instrument based on the defined framework to perform an information security culture assessment.

Chapter 4 will aim to address the third research question, which relates to the development an information security framework that can serve as the

foundation for an information security culture framework and assessment instrument.

PART II

CHAPTER 4

A Framework for Information Security

4.1 INTRODUCTION

Chapter 4 describes the development of a comprehensive framework for *information security*. This framework is developed to serve, in turn, as the foundation for an *information security culture* framework. This contributes in addressing the third research question, namely to identify what an information security culture framework comprise of in order to cultivate information security culture. One should first understand what an information security framework entails before trying to define what an information security culture framework is. The author will therefore attempt to identify those components of information security that could influence information security culture in an organisation. Based on these components a suitable framework for information security culture will be developed in Chapter 5.

In this chapter then, a comprehensive list of information security components is compiled. The chapter concludes with the Comprehensive Information Security Framework (CISF) that incorporates the information security components identified through the investigation of existing information security components.

4.2 INFORMATION SECURITY APPROACHES

Approach, also defined as method, is an “orderly arrangement of ideas” (Oxford Dictionary 1983, 2005). If one applies this definition, an information security approach is the arrangement or structuring of information security components to implement information security in an effective manner to mitigate risks in an organisation. An information security component is considered as a part of an information security approach that contributes to the implementation and maintenance of information security. In other words, determining what must be implemented or considered by the organisation in

terms of information security – such as an information security policy, risk assessments, technical controls and information security awareness.

Researchers use different terminology when referring to information security components. The term “control” is used by ISO/IEC 17799 (2005), Tudor (2006) as well as Sherwood, Clark and Lynas (2005), while McCarthy and Campbell (2001) use both “control” and “component”. For the purposes of this research study, the term “component” will be used.

Various researchers propose different approaches towards information security that an organisation can use to assist management in implementing information security components. They structure information security components in what can be referred to as an information security architecture, framework, model or standard.

- Architecture: Tudor (2006), Sherwood, Clark and Lynas (2005) and Eloff and Eloff (2005) use the terminology “architecture”. Tudor (2006) explains that an information security architecture provides the organisation with an understanding of the requirements for a strategic plan for security and combines technical, practical and cost-effective components to achieve an appropriate level of security. An architecture is defined as “a structure or systemisation of knowledge” (Oxford Dictionary 1983, 2005). An information security architecture is therefore the structure in which is presented the information security components that can be interpreted as knowledge.
- Model: McCarthy and Campbell (2001) refer both to a model and an architecture when structuring their definition of information security components. A model is defined as a “proposed structure” (Oxford Dictionary 1983, 2005), which relates to the definition of an architecture.
- Framework: Trček (2003) uses the word framework for information security components that manage information systems security. The Oxford Dictionary (1983, 2005) defines a framework as a structure upon or into which contents can be put and further relates it to thoughts that are directed for a purpose. An information security framework can therefore be

seen as a structure into which information security components are put for the purpose of minimising risks to an acceptable level.

- Standard: Standard is defined as a document that specifies (inter)nationally agreed properties, for instance a British Standard (Oxford Dictionary 1983, 2005). The ISO/IEC 17799 (2005) British Standard defines components that can be used to mitigate risks to information assets. Thus, the components are structured in a standard to be used by an organisation to minimise threats to information assets.

For the purpose of this research, the term "framework" is preferred. In order to define a comprehensive framework for information security, the next section provides a description of existing information security approaches to arrive at a comprehensive set of information security components. The latter can be utilised to direct employee behaviour in all required facets of information security and cultivate an acceptable level of information security culture. The components can also be used to set key behaviour traits. Ultimately they will serve as a guide in developing an information security culture assessment tool with which to assess whether the level of information security culture contributes to or negatively impacts on the protection of information assets.

4.2.1 Existing information security approaches

For the purpose of this research it is important to consider information security approaches that comprise of components that could influence employee behaviour to ultimately aid in cultivating an information security culture. Components (people components) that could influence employee behaviour are for instance an awareness programme that aids employees to understand what is required of them with regard to the protection of information assets. An information security awareness programme is seen as the stepping stone in creating an information security culture (Grant 2005). Other examples are trust and change management.

People components alone are not sufficient for a comprehensive information security framework. Process and technology components should also be

addressed in the framework to ensure that it is holistic (Eloff & Eloff 2005). Furthermore, the framework proposed in this research study should not only relate to a specific technology environment such as an e-business or the IT department operations, but should also apply to the business as a whole, making it scalable to different environments and organisations. The next section provides an overview of information security approaches and indicates which approaches are applicable in the identification of components for the information security framework defined for the purpose of this research study.

The ISO/IEC 17799 (2005), PROTECT (Eloff & Eloff 2005), the Capability Maturity Model (McCarthy & Campbell 2001), the Standard of Good Practice (SOGP 2003) from the ISF (ISF 2003) and Tudor (2006) all address the people component, which is important for the context of this research study. ISO/IEC 17799 (2005) addresses awareness while PROTECT (Eloff & Eloff 2005) includes ethical and culture components. The Capability Maturity Model (McCarthy & Campbell 2001) emphasises privacy and Tudor (2006) mentions trust. These frameworks incorporate not only people components, but also technology and process components, which could aid in defining a comprehensive framework for information security to cultivate information security culture.

Other information security approaches (Rees, Bandyopadhyay & Spafford 2003; Sherwood; Clark & Lynas 2005; Van der Raadt, Soetendal, Perdeck & Van Vliet 2004; Trček 2003; Siponen & Willison 2007; SSE-CMM 2008) also propose frameworks to implement information security, but these do not relate specifically to the context of this research study. The version of the Capability Maturity Model referred to as Systems Security Engineering Capability Maturity Model (SSE-CMM) focuses specifically on the development of secure products across the products system life cycle (SSE-CMM 2008). The framework proposed by Trček (2003) is specifically designed for an e-business environment. Similarly, Rees et al. (2003) propose the Policy Framework for Interpreting Risk in E-Business Security (PFIRES), thus

highlighting the importance of an information security policy. Their framework is however specific to the e-business environment.

Sherwood, Clark and Lynas (2005) base their framework on the "Sherwood Applied Business Security Architecture" (Sherwood 2006). The focus is on designing a secure environment across systems considering the business environment. It does not relate to the people component, but focuses on the process and technology layers. The same applies to the Zachman framework (Zachman 2008) that also focuses on the provision of a framework for the development of systems.

Van der Raadt et al. (2004) performed an investigation in organisations to understand how the organisations interpret the concept "framework" (referred to as "architecture" by the researchers). Although they did not propose a framework as such, their work illustrates that organisations differ in maturity of implementing IT and system frameworks, and that each organisation values different critical success factors, depending on its business.

Next, the information security approaches relating to information security frameworks that could be used to identify the components of an information security culture framework will be discussed in order to compile a comprehensive list of information security components. These approaches (ISO/IEC 17799 (2005); PROTECT (Eloff & Eloff 2005); Capability Maturity Model (McCarthy & Campbell 2001); ISA (Tudor 2006) and SOGP (2003)) consider technical, process and people components, yet with a specific focus on the people component. The exercise will aid the author in compiling a comprehensive information security framework that can be used influence employees to protect information assets in a more secure manner.

4.2.2 ISO/IEC 17799 and ISO/IEC FDIS 27001

The ISO/IEC 17799 (2005) security standard takes the form of guidance and recommendations and is intended to serve as a single reference point for

identifying the range of controls needed for most situations where information systems are used. The standard consists of the following 12 components:

- Security policy that aims to provide management direction and support for information security, including laws and regulations.
- Organisation of information security that constitutes the process implemented to manage information security within the organisation.
- Asset management that focuses on asset inventories, information classification and labelling.
- Human resources security that considers permanent, contractor and third party user responsibilities to reduce the risk of theft, fraud and misuse of facilities. This section also includes awareness, training and education of employees.
- Physical and environmental security controls that allow only authorised access to facilities and secure areas.
- Communications and operations management that focus on the correct and secure operation of information-processing facilities such as segregation of duties, change management, malicious code and network security.
- Access components that manage user access to information and include clear desk principles, network access controls, operating system access controls, passwords and teleworking.
- Information systems acquisition, development and maintenance that ensure the security of user-developed and off-the-shelf products.
- Information security incident management that ensures that incidents are communicated in a timely manner and corrective action is taken.
- Business continuity management that focuses on business continuity plans and the testing thereof.
- Compliance in terms of statutory, regulatory or contractual requirements or obligations, laws, audit and organisational policy.
- Risk assessment and treatment to identify, quantify, prioritise and treat risks posed to information assets.

The ISO/IEC FDIS 27001 (2005) is considered as part two of ISO/IEC 17799 (2005) and proposes an approach of continuous improvement through a

process of establishing, implementing, operating, monitoring, reviewing, maintaining and improving the organisation's information security management system. These two international standards are considered a single encompassing approach since ISO/IEC 17799 details the components of information security and ISO/IEC 27001 outlines the approach required to implement and manage them.

4.2.3 PROTECT

The research conducted by Eloff and Eloff (2005) introduced a comprehensive approach towards information security, namely PROTECT, which is an acronym for Policies, Risks, Objectives, Technology, Execute, Compliance and Team. PROTECT is aimed at addressing all aspects of information security. It involves an approach that considers various and well-integrated controls in order to minimise risk and ensure effectiveness and efficiency in the organisation. The seven components of PROTECT are aimed at implementing and managing an effective information security programme from a technology to a people perspective. They are summarised below:

- The *policy* component includes information security policies, procedures and standards, as well as guidelines for maintaining these.
- *Risk* methodologies such as CRAMM and Octave, as well as automated tools to identify system vulnerabilities, are covered in the risk component.
- *Objective* refers to the implementation of controls by considering the risk environment of the organisation and not implementing more or less controls than what is required to meet the objective of a secure environment.
- *Technology* components refer to hardware, software and systems product components of the IT infrastructure and, where possible, the use of certified products.
- Information security components need to be established, maintained and managed. *Execute* therefore refers to a proper information security management system environment.
- The *compliance* component covers both internal compliance with the organisation's policies and external compliance with information security

expectations set by outside parties to the organisation. This component also includes international codes of practice, legal requirements and international standards.

- *Team* refers to the people component, i.e. all the employees of the organisation, where each has a responsibility towards securing information. The objective is to create a security aware workforce that will contribute to an improved information security culture.

4.2.4 Capability Maturity Model

The Capability Maturity Model (McCarthy & Campbell 2001) approach provides components used to protect information assets against unauthorised access, modification or destruction. The framework is based on a holistic view of information security and encompasses seven main components, namely:

- Security leadership by means of an executive level security representative and an information security strategy.
- A security programme with defined roles and responsibilities for information security tasks.
- Security policies, standards and guidelines that are used to direct the implementation of information security.
- Security management that constitutes day-to-day operations and monitors users and technology.
- User management that focuses on awareness of policies and manages user profiles.
- Information asset security that encompasses the technology aspects of information security, such as configuring a secure firewall and network.
- Technology protection for the environment and continuity thereof, which focuses both on business continuity and disaster recovery.

The objective of this framework is to start from the top on a strategic level and work down to the technology levels guided by the direction provided by the strategic levels. In implementing information security, the framework is used to assess the current information security capability and risks and to architect the appropriate solution in order to mitigate risks. The solution, as well as

monitoring capabilities, is subsequently implemented and integrated with current processes.

4.2.5 Information Security Architecture (ISA)

Tudor (2000, 2006) proposes an Information Security Architecture (ISA) approach that is comprehensive and flexible enough to protect an organisation's assets against threats. This work highlights five components that are used to understand the risk environment in which organisations operate in order to evaluate and implement controls to mitigate such risks. Country regulations are also considered to ensure that each organisation's confidential information is protected accordingly. The components encompass the following aspects of process as well as technology in order to address organisations' security needs:

- Security organisation and infrastructure with defined roles and responsibilities, as well as executive sponsorship.
- Security policies, standards and procedures that are supported by management.
- Security baselines and risk assessments across platforms, databases, applications and networks, providing an adequate budget for resources.
- Security awareness and training programmes, as well as an environment of trust.
- Compliance testing and audits to monitor the effectiveness of the security programme.

4.2.6 Standard of Good Practice for Information Security (SOGP)

The Standard of Good Practice for Information Security (SOGP 2003) is based on the input of 25 member firms that belong to the ISF. Their framework is perceived as one of the most comprehensive and integrated in terms of information risk management (SOGP 2003). The standard or framework consists of five component categories namely security management; critical business applications; computer installations; networks;

and systems development. Each component category involves a number of components, in total 132.

Amongst other components, it addresses the importance of management commitment to information security in order to direct information security in an organisation. It also addresses the importance of information security awareness for the different job levels in an organisation in order for employees to understand their personal information security responsibilities. The SOGP also emphasises the importance of protecting personal information to prevent it from being used improperly and to comply with legal and regulatory requirements. The framework furthermore addresses technical components such as incident management and intrusion detection.

4.3 INVESTIGATION OF INFORMATION SECURITY APPROACHES

A comprehensive list of components was compiled from the ISO/IEC 17799, PROTECT, the Capability Maturity Model, ISA and SOGP. The components in Table 4.1 were selected from each information security approach where a component was depicted as a key focus area. By highlighting these existing information security components, an attempt is made to compile an "ideal" list of components which, in the opinion of the author of this thesis, could aid in directing employee behaviour.

Components relating to information security concepts (e.g. trust and privacy), as well as for instance processes or activities (e.g. asset and incident management) are listed. The objective is to list all the components and to further categorise and explain the relationship between the components when developing the comprehensive framework for information security. The components are listed in no specific order and although some overlapping might be evident (e.g. user awareness and education and training), the list is used further on to group similar components together. For each component that was addressed in a specific approach, an inclusion tick ("✓") is given.

Table 4.1 Components of an information security approach

	Information security components	ISO 17799 (2005)	Eloff and Eloff	McCarthy and Campbell	Tudor	SOGP
1	Sponsorship	✓	✓	✓	✓	✓
2	Strategy	X	X	✓	X	X
3	IT governance	X	X	X	X	✓
4	Risk management	✓	✓	✓	✓	✓
5	ROI (Return on investment) /Metrics /Measurement	X	✓	✓	X	✓
6	Programme organisation	✓	✓	✓	✓	✓
7	Legal and regulatory components	✓	✓	✓	✓	✓
8	Security policies, procedures, standards and guidelines	✓	✓	✓	✓	✓
9	Certification	✓	✓	X	X	X
10	Code of / best practice	✓	✓	✓	✓	✓
11	Monitoring and audit	✓	✓	✓	✓	✓
12	Compliance	✓	✓	✓	✓	✓
13	User awareness	✓	✓	✓	✓	✓
14	Education and training	✓	✓	✓	✓	✓
15	Ethical conduct	X	✓	X	X	X
16	Trust	X	X	X	✓	X
17	Privacy	X	X	✓	X	✓
18	Asset management	✓	✓	X	✓	✓
19	System development	✓	✓	✓	X	✓
20	Incident management	✓	X	✓	X	✓
21	Technical operations	✓	✓	✓	✓	✓
22	Physical and environmental components	✓	✓	✓	✓	✓
23	Business continuity planning (BCP)	✓	X	✓	✓	✓
24	Change management	✓	✓	X	✓	✓

4.3.1 Defining the information security components

The different components listed in Table 4.1 are defined below.

- Sponsorship: This component refers to an executive sponsor that supports the information security strategy and provides guidance with regard to information security in the organisation (Schiesser 2002; SOGP 2003). An executive sponsor will typically sit in on the executive board meetings and present information security as an item of the agenda.

- Strategy: An information security strategy involves the creation of a strategic vision and plan to address information security risks, but also to meet business objectives (CISA 2005; Sherwood, Clark & Lynas 2005). The information security strategy should be linked to the organisational and IT strategy to ensure that the organisation's objectives are met both in the short and the long term.

- IT governance: Von Solms (2006) explains that the development of information security over a period of time started with a technical wave focussing on technical components, then a management wave concentrating on policies and a third wave where the focus was on institutional components such as awareness and culture. He argues that the next wave will be characterised by corporate governance and specifically information security governance, which is an integral part of good IT and corporate governance (Von Solms 2005). IT governance is concerned about the policies and procedures that define how an organisation will direct and control the use of its technology and protect its information (Posthumus & Von Solms 2005).

  Corporate governance can be explained as the direction and management of a set of policies and internal controls in an organisation. Information security governance relates to the commitment of the organisation's executive board to information security and the management of information security through policies, procedures, processes, technology, compliance

enforcement mechanisms, as well as awareness initiatives for users (Von Solms 2006).

- Risk management: Risk management is a process for resolving risk. The process includes risk assessment to define the risk, and risk control to resolve the risk (Hall 1998:5). Information security risks such as the threat of viruses, hackers or natural disasters need to be identified and the control implemented by considering a cost benefit analysis.

- ROI /metric /measurement: Return on investment in terms of information security refers to spending resources. These resources could be money, time and effort so as to gain something – for instance, more secure systems or fewer information security incidents. In order to illustrate a return on investment, the information security efforts have to be measured using metrics (Sherwood, Clark & Lynas 2005: 79-81). The Oxford Dictionary (1985, 2005) defines metrics as a decimal measuring system. Applying this definition to information security one would for instance aim to measure the number of incidents, the time taken to resolve incidents or the number of users who attended the information security induction presentation. Many organisations are turning to metrics to evaluate the effectiveness of their information security programmes (Witty & Hallawell 2003).

- Programme organisation: Programme organisation refers to the information security organisational design, composition and reporting structures (e.g. centralised or decentralised management of security). It also incorporates the roles and responsibilities, skills and experience, and resource levels committed to the enterprise's security architecture (McCarthy & Campbell 2001). Information security responsibilities within the organisation should be allocated in terms of its information security policy. An example of an information security role is the Information Security Officer who is responsible for the management of information security or the network specialist who will ensure that the network is configured in a secure manner. Organising and formally defining the

information security roles will aid in providing a clear definition of the department's hierarchy and authorities (CISA 2005: 84).

- Legal and regulatory components involve compliance with legislation. Different pieces of national and international legislation need to be considered for information security – such as the Health Insurance Portability and Accountability Act (HIPAA) (Bresz 2004); the Sarbanes-Oxley Act (Donaldson 2005); the King Report II (King II); Electronic Communications and Transactions Act (ECTA) (2002); and the Promotion of Access to Information Act (PROATIA) (2000).

- Security policies, procedures, standards and guidelines: ISO 17799 defines a policy as the "overall intention and direction as formally expressed by management". In other words, it is a document detailing what management expects of employees in terms of protecting information assets and is usually not technology specific. An example is an Information Security Policy stating that access should be controlled. A procedure provides the detailed steps of a component mentioned in a policy, for instance the process of granting access and distributing passwords. A standard details the minimum requirements, for instance that a password must be at least 8 characters long and consist of alpha-numeric characters. A guideline is a document that assists management in the implementation of information security. Organisations can use international standards such as ISO/IEC 17799 (2005) as a guideline when compiling the above documents.

- Certification: Organisations can certify against international standards such as ISO/IEC 17799 (2005). The Financial Services Authority (FSA) recommends certification against ISO/IEC 17799 (2005) as it aids in meeting many regulatory requirements relating to information security.

- Best practice or code of practice: International standards such as the Standard of Good Practice from the Information Security Forum (ISF 2008), the Control Objectives for Information Technology (COBIT) from the

Information Systems Audit and Control Association (ISACA) (COBIT 2004, ISACA 2008) and ISO/IEC 17799 (2005) are examples of best practices that can be used by organisations to implement and manage information security. These standards can guide management to mitigate the information security risks posed by the information security components identified in the comprehensive information security framework defined later in this chapter.

- Monitor and audit: Organisations need to monitor their compliance with regulations as these could change over time. New regulations could be approved by government or the organisation's business could change, resulting in additional regulations that have to be complied with. Furthermore, since users may not always comply with the requirements, they need to be monitored. Monitoring can be conducted as part of the information security function responsibilities, internal audit, external audit and also by means of self-assessments. Information security auditing is necessary to ensure that the policies, processes, procedures and controls are in line with the objectives, goals and vision of the organisation (Vroom & Von Solms 2004).

- Compliance: Compliance relates to ensuring that the organisation complies with international and national laws as well as industry regulations pertaining to the protection of information (Sherwood, Clark & Lynas 2005: 542). It is essential to measure and enforce compliance (Von Solms 2005), and both technology and employee behaviour (Vroom & Von Solms 2004) should be monitored to ensure compliance to information security policies and to respond effectively and timely to incidents that are detected.

- User awareness: McIlwraith (2006) believes that awareness is the "single most effective thing an information security practitioner can do to make a positive difference to their organisation". Awareness can be explained as the different activities that the organisation deploys to reinforce information security requirements and responsibilities required by the information

security policy (SOGP 2003). E-mail communication or posters can for instance be used to raise awareness about information security requirements.

- Education and training: ISO/IEC 17799 (2005) states that "all employees of the organisation and, where relevant, contractors and third party users should receive appropriate awareness training and regular updates in organisational policies, procedures, as relevant for their job function". Users must therefore receive training, which could include induction training presentations, Web-based training or group discussions.

- Ethical conduct: Hellriegel, Slocum and Woodman (1998:19) define ethics as the values and rules that distinguish right from wrong. For example, employees should not talk about confidential information in public places.

- Trust: Trust is important when implementing information security. It aids in providing confidence to information users when making decisions. Flowerday and Von Solms (2006) remark that "confidence in information security management requires trust and trust requires information security to help safeguard it".

  Martins and Van Der Ohe (2002) defines trust as "the process in which a trustor relies on a trustee (a person or group of people) to act according to specific expectations that are important to the trustor without taking advantage of the trustor's vulnerability". When implementing the information security components, management must be able to trust employees to adhere to information security policies, while employees must be able to trust management to illustrate commitment to information security (trust is seen as the primary attribute of leadership) (Robbins 1997: 257). A trusting relationship should also be established between trading partners and clients who could contribute to the organisation's reputation. One possible way of establishing such a relationship could be for the organisation to illustrate that information and assets are secured and that employees comply with requirements.

- Privacy: Privacy is an essential issue of trust. Without privacy there is no trust (Borking 2006; Sartor 2008). When implementing information security privacy, both employees and customers must be considered and controls must be implemented to protect the personal identifiable information of an individual (ISACA 2005, SOGP 2003). An identification number, name and surname or address are examples of personal identifiable information. The organisation has to ensure that adequate controls are in place to protect personal information of employees, contractors, customers and third parties.

- Asset management: Asset management relates to the protection of organisational assets, which includes the identification of assets and maintaining an inventory thereof. It also incorporates the protection of information by classifying it based on the degree of sensitivity and criticality (ISO/IEC 17799:2005).

- System development: This component addresses security in system files and the development of new application system software. It also ensures that the change control process followed considers security (ISO/IEC 17799:2005).

- Incident management: Incident management is the process used to identify, respond to and monitor information security incidents (ISO/IEC 17799:2005). An information security incident could be a virus affecting the organisation's network, a stolen laptop or sharing of a password between employees.

- Technical operations: Technical operations refer to the technology used to protect the environment and information assets for instance anti-virus software, firewalls and network configuration, capacity and configuration management (ISO/IEC 17799:2005).
- Physical and environmental components: Physical and environment components relate to the protection of the security perimeter and secure

areas such as a server room by, for instance, access cards. It also includes protection against environmental threats such as fire, for which a fire extinguisher is needed (ISO/IEC 17799:2005).

- Business continuity planning (BCP): Business continuity involves the prevention and mitigation of disruption, as well as the recovery of the business (processes, people and technology) from a disruption (ISACA 2003). A disruption could be a power failure or an earthquake affecting the LAN connectivity between offices. Disaster recovery is part of business continuity. Schiesser (2002) defines disaster recovery as "a methodology to ensure the continuous operation of critical business systems in the event of widespread or localised disasters to an infrastructure environment". An organisation has to identify its critical business systems and ensure that there is a plan in place to recover these systems. The plan could for instance involve another site where the environment is duplicated, and the making and off-site storage of such backups.

- Change: Implementing the information security components will institute change in the organisation's processes and will influence the way people conduct their work. An important truth is that organisations do not change, but people do, and therefore people change organisations (Verton 2000). Information security changes in the organisation need to be accepted and managed in such a way that employees are able to successfully incorporate such changes into their work. As employees incorporate/internalise the information security components, their behaviour will over a period of time become more acceptable in terms of protecting information assets. The change in behaviour relating to compliance and the protection of information assets is important when the degree of success of the implementation of the components is to be measured.

4.3.2 Discussion of the investigation into information security approaches

Based on an investigation of the different approaches, the ISO/IEC 17799, McCarthy and Campbell's framework and the SOGP are the most comprehensive in addressing the extent of information security components in Table 4.1. Ethical conduct and trust are not included in either of these approaches, although both components are considered by various other researchers (Donaldson 2005; Flowerday & Von Solms 2006; Trompeter & Eloff 2001; Eloff & Eloff 2005; Tudor 2000) when addressing information security in an organisation.

The approach put forward by Eloff and Eloff (2005) suggests a holistic set of components to consider and focuses mainly on providing a standardised approach for the management of an information security programme. It is the only approach that mentions ethical values. Employees need to incorporate ethical conduct or behaviour relating to information security as part of their everyday life in the organisation (Trompeter & Eloff 2001). According to Baggett it is the responsibility of management and the board to develop and distribute corporate codes of conduct that should cover both commercial and social responsibilities (Baggett 2003). Ethical conduct, for example not copying organisational software at home or using the Internet for personal gain during working hours, needs to be enforced as the accepted way of conduct in the work environment for the correct information security culture to emerge eventually. Although the Eloff approach (Eloff & Eloff 2005) is very comprehensive, it does not mention aspects such as business continuity or incident management. These could however be covered under the policy and procedures component.

Only Tudor mentions trust in his approach. According to Von Solms, information security is arguably the most important issue for instilling trust in an IT environment (Von Solms 2000). If management trusts its employees and the employees trust management, it is easier to implement new procedures and guide employees through changes of behaviour regarding information

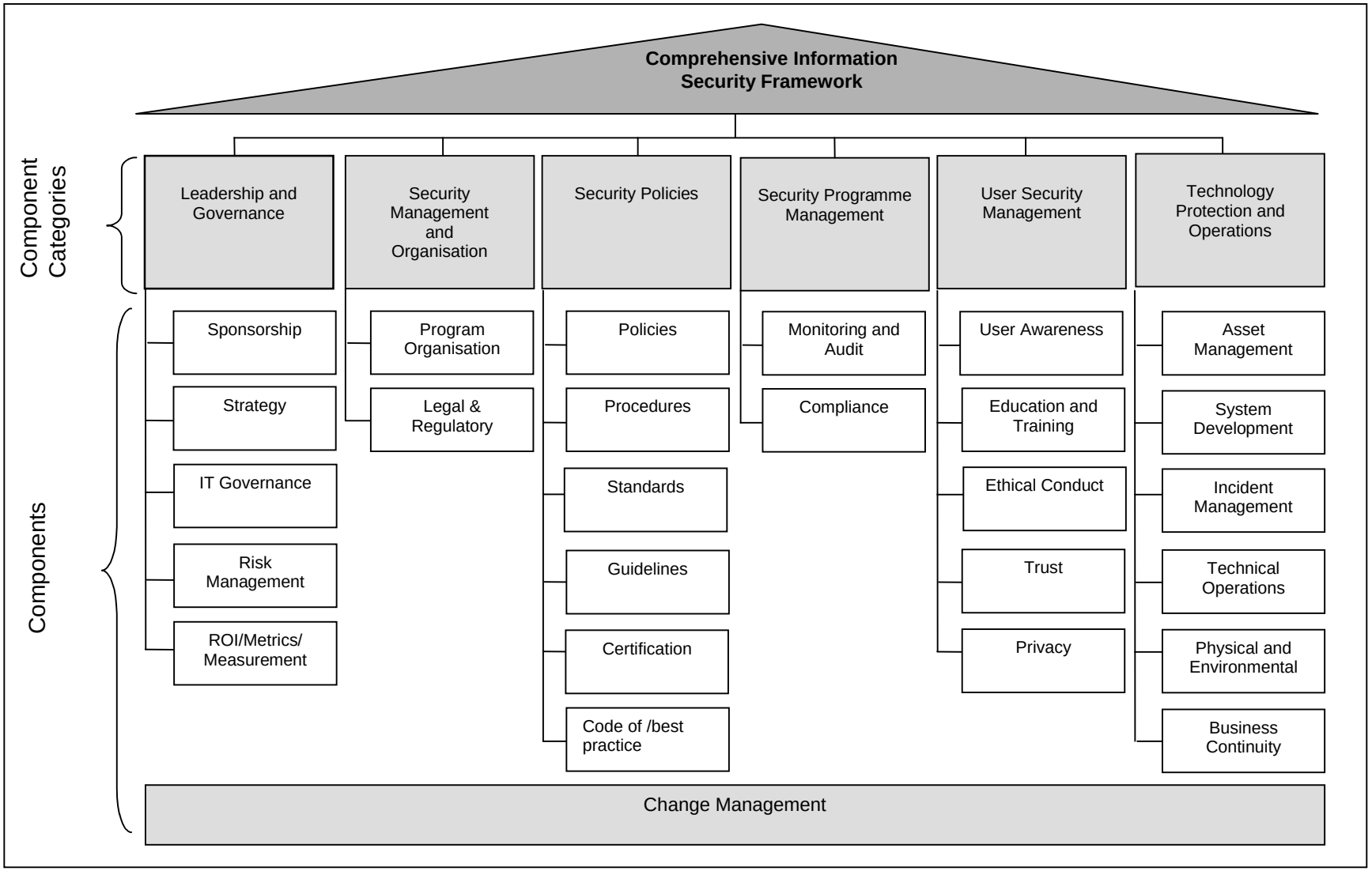
security. Corporate governance, together with ethical considerations and trust, would need to be incorporated into the approach that an organisation uses if it is to provide a comprehensive set of information security components to deal with its risks.

All the information security approaches consider the component of change management. However, they address it from the perspective of managing technology and process changes and not as the management of people behaviour to aid employees in changing their attitudes and perceptions regarding the protection of information.

4.4 PROPOSED INFORMATION SECURITY FRAMEWORK

The proposed framework for information security, the Comprehensive Information Security Framework (CISF) (Figure 4.1), can be used by an organisation as a starting point to develop guidelines and implement controls for addressing identified risks.

Figure 4.1 Comprehensive Information Security Framework (CISF)



The components of CISF are structured in six component categories comprising of the components listed in Table 4.1. The components are depicted in the categories to illustrate similar concepts that are addressed by the various components. Furthermore components that are of a strategic and managerial nature are depicted on the left side of the framework illustrated in Figure 4.1, thus providing direction to the technical implementation and protection of assets on the right side of the framework. Change management is depicted at the bottom of the framework so as to illustrate that it should be considered across all the component categories. The rationale for grouping the components is further based on the framework proposed by McCarthy and Campbell (2001), whereby for instance the technology components are grouped and the related management and strategic components are grouped.

- Leadership and Governance are of a strategic nature and provide direction for the implementation of the components in the other categories. Without sponsorship and strategy, the appropriate direction for the remainder of the components cannot be provided. Risk management being part of this category serves as the input for defining the level of protection required and provides direction in terms of strategy. For instance, the risk of threats to information in a bank is much higher as opposed to a retail store. Hence the information security strategy of these organisations will be different based on the risk profile of each. Metrics and measurement also provide input to the direction as they aid the organisation in assessing the overall success of the information security function and to identify remedial actions.

- Security Management and Organisation comprise of components that aid in managing information security in the organisation and advise how to structure the information security office by also considering regulatory requirements. The components grouped in this category relate specifically to the processes and structures of the information security function.

- The Security Policy category consists of the documented requirements defined by the organisation and (inter)national standards or guidelines to

direct employee behaviour. The policies should consider component categories such as legal considerations and must be implemented in the organisation by means of effective processes that also include compliance monitoring thereof. Security policies are categorised on their own as they encapsulate the direction provided by the previous categories and are used to provide direction for the categories on the righthand side of the framework. They could perhaps also fall within the security management and organisation category, but as they have such a huge influence on the manner in which controls are deployed and what is expected of employees, they are categorised separately.

- Security Programme Management refers to the components that are deployed to ensure the effective management of information security. Monitoring and compliance as well as auditing are included in this component category to manage the security programme.

- The User Security Management category involves those components that relate to the employees in the organisation and ways of directing their behaviour. As such, processes like education and training, as well as concepts like trust are depicted in this category as they relate specifically to the people component of information security.

- Technology and operations involve the technical and physical mechanisms implemented to secure an IT environment. All components relating to the technology component of information security are grouped together. When implementing the information security framework, the technology controls applicable to the organisation's environment and identified risks must be implemented. These include asset management, system development requirements, incident management, technical operations such as network security, and physical, environment and business continuity controls.

4.5 CONCLUSION

The aim of Chapter 4 was to develop a framework for information security. Four information security approaches were discussed and investigated in terms of information security components. Finally the CISF was constructed, providing a comprehensive and complete framework to define information security in an organisation and ultimately cultivate a culture of information security.

Chapter five sets out to develop a framework for information security culture and uses the CISF as a foundation to ensure that all the information security components are considered to cultivate an acceptable level of information security culture.

CHAPTER 5

A Framework for Information Security Culture

5. 1 INTRODUCTION

Chapter 5 defines a framework for information security culture, which can be used to cultivate information security culture in an organisation. Chapter 5 therefore addresses the third research question stated in chapter 1, which relates to identifying what an information security culture framework comprise of in order to cultivate information security culture. The Information Security Culture Framework (ISCF) is developed by considering the Comprehensive Information Security Framework (CISF) developed in Chapter 4. The influence of organisational behaviour and organisational culture on the information security components is also considered with an aim to develop the ISCF. The framework can furthermore serve as the basis for designing an information security culture questionnaire that can be used to assess the status of the information security culture.

5. 2 A FRAMEWORK FOR INFORMATION SECURITY CULTURE

Organisations require a comprehensive framework to cultivate an acceptable level of information security culture (Helokunnas & Ilvonen 2004) – one that specifically incorporates human behaviour so as to address the threat that such behaviour poses to the protection of information assets. This framework could assist management in identifying the relevant controls and their impact on employees' perception and behaviour.

The framework for information security culture that is proposed in this research study helps organisations to understand how to establish an information security culture that can help them to minimise the risks posed by employee behaviour when information assets are used.

The ISCF is constructed by systematically considering the various fields of knowledge that affect an information security culture. Research (Connolly 2000; Le Grand & Ozier 2000) indicates that an information security culture is part of the overall organisational culture that develops based on the organisational behaviour exhibited by employees (Hellriegel, Slocum & Woodman 1989: 549). Organisational behaviour must therefore be taken into account, as well as the information security components defined in Chapter 4. The interaction between these fields of knowledge is illustrated in the following paragraphs and enables the construction of an information security culture framework.

5.2.1 Information security culture and organisational culture

Probably the best-known definition of organisational culture is “the way things are done here” (Lundy & Cowling 1996). Organisational culture can be seen as the personality of the organisation (Robbins 2001) and it is the social glue that binds the members of an organisation together (Kreitner & Kinicki 1995: 532).

An organisational culture develops on the basis of certain activities in the organisation, such as the vision of management and the behaviour that employees exhibit on an individual, group and organisational level (tier) (Hellriegel, Slocum & Woodman 1998; Robbins 2001). The organisational culture that develops on the basis of the exhibited behaviour is evident in artifacts (locked door), values (‘employees are valuable assets’) and basic assumptions (‘the Information Technology department is responsible for the security of CIS’) (Schein 1985: 14).

According to Robbins (2001), organisational behaviour is about what people do in an organisation and how their behaviour affects the performance of the organisation. The term also incorporates employee attitude and how it relates to the behaviour of employees in the organisation (Hellriegel, Slocum & Woodman 1998: 4).

An information security culture develops due to the information security behaviour of employees in the same manner that an organisational culture develops due to the organisational behaviour of employees in the organisation (Martins 2002; Martins & Eloff 2002; Robbins, Odendaal & Roodt 2003: 15; Hellriegel, Slocum & Woodman 1998: 594). An information security culture is therefore based on the interaction of employees with information assets and the security behaviour they exhibit.

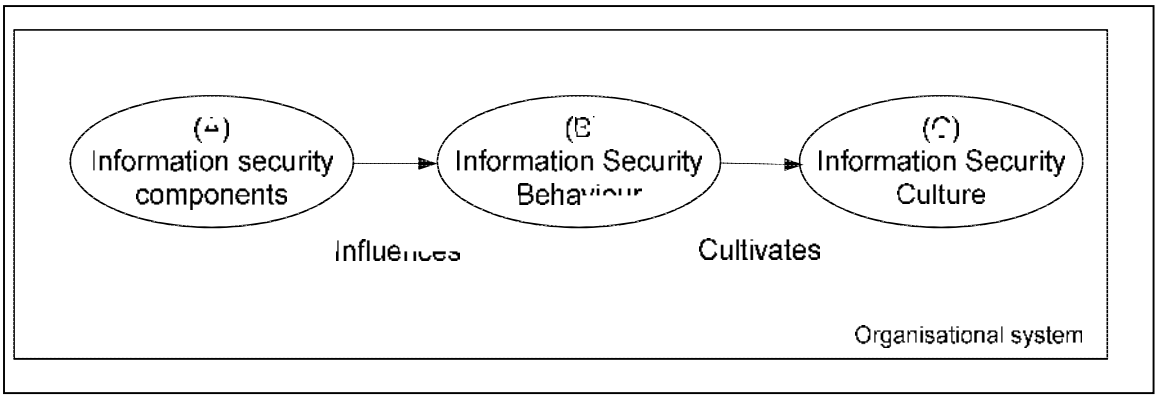
5.2.2 The interaction between information security, behaviour and culture

The interaction between information security components (e.g. a policy and the behaviour of employees) has an impact on the information security culture that emerges. The next few paragraphs explain this interaction by way of three figures that build upon one another to finally construct the ISCF. The figures will be referred to as level 1 (Figure 5.1), level 2 (Figure 5.2) and level 3 (Figure 5.3).

5.2.2.1 Level 1 - Influencing information security behaviour and cultivating an information security culture

Figure 5.1 (level 1) illustrates that information security components (A) are implemented in the organisation. These components can be seen as the input that *influences* information security behaviour in the organisation (B). Implementing the information security components impacts on the interaction of employees with information assets, and employees consequently exhibit certain behaviour referred to as information security behaviour.

Figure 5.1 Level 1 - Influencing information security behaviour and cultivating an information security culture



The objective is to instil information security behaviour that is conducive to the protection of information assets based on the organisation's information security policies and code of ethics. Such behaviour could involve the reporting of security incidents, adherence to a clear desk policy or the secure disposal of confidential documents. In time, this security behaviour evolves as the way that things are done in the organisation and an information security culture is therefore established (cultivated) (C). A culture is thus promoted in which ensuring the security of information is accepted as the way things are done.

To illustrate the interaction between A, B and C, the following example is used. The information security policy, one of the information security components, is used to provide employees with a clear understanding of management's direction and support for information security (ISO/IEC 27001 2005). According to Whitman and Mattord (2003), the objective of a policy is to influence the decisions, actions and behaviours of employees. It further specifies what behaviour is regarded as acceptable and what not. For instance, the information security policy may state that a laptop must be physically secured at all times. The statement in the policy is aimed at directing employee behaviour to protect both the physical asset and the data saved on the laptop. The objective is to influence the employee's behaviour when interacting with the laptop to ensure the protection thereof. Without this statement and its enforcement, employees could leave their laptops

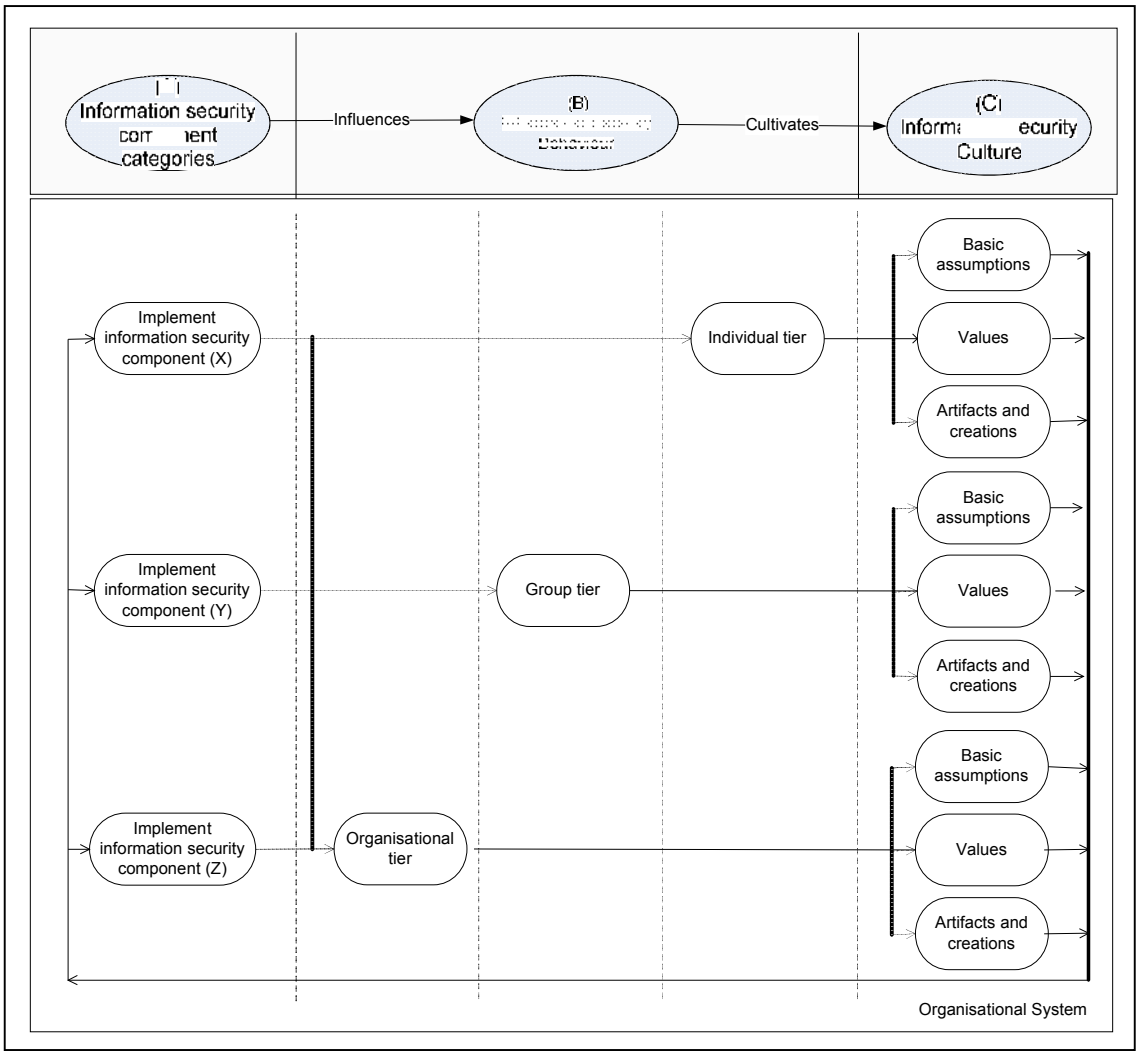
unsecured. Therefore, without information security components to direct and influence employee behaviour, employees could well interact with information assets in ways that would introduce risk. In time, such potentially harmful behaviour could unfortunately give rise to a culture where neglect is regarded as acceptable.

To administer a positively acceptable level of information security, organisations should ensure that a comprehensive and adequate set of information security components is implemented. This set of information security components aids in addressing threats on the technical, process and people levels, in other words threats that would negatively influence the establishment of an acceptable information security culture within the organisation. Organisations should furthermore ensure that employee interaction is in line with the requirements of the information security policy. These requirements could involve actions such as making back-ups to the server on a daily basis, password protect information on removable media or the deletion of unsolicited e-mails with attachments.

5.2.2.2 Level 2 - Influencing information security behaviour and cultivating an information security culture

Figure 5.2 explains the interaction between information security component categories, information security behaviour and information security culture. It illustrates that the set of information security components can be grouped into categories of components (A) that are implemented by the organisation. (These categories are referred to as X, Y and Z in the figure.) The components are implemented by the organisation on the individual, group or organisational tier of information security behaviour (B). As such, information security behaviour is influenced and exhibited on each behavioural tier.

Figure 5.2 Level 2: Influencing information security behaviour and cultivating an information security culture



The *individual* tier relates to individuals in the organisation who display characteristics that may influence their behaviour at work (Robbins, Odendaal & Roodt 2003: 44-45). These characteristics could involve biographical features such as age or marital status; personality characteristics; inherent emotional frameworks; values; and attitudes and basic assumptions (Robbins 2001). They could affect the behaviour of individuals regarding compliance with information security policies. For example, if one considers two types of personalities (A and B), there could be a distinct difference in the way they comply with the information security policy (Robbins 1998: 65). Type A employees emphasise quantity over quality. They work fast and illustrate their competitiveness by working long hours, but often make poor decisions

because they make them too fast. Type B employees focus on quality and never suffer from a sense of time urgency. Type A employees, again, might be too hasty to select a strong password. They might share passwords to easily access information rather than to wait for the authorised user to return to access a system. Type B might think twice before making a decision and would probably take a few seconds more to decide on a stronger password. Information security components that positively influence the individual's information security behaviour should therefore be implemented on the individual tier.

The *group* tier focuses on the behaviour of people in groups and on the ways in which these groups function (Robbins et al. 2003: 173-186). It is important for management to consider employees as members of a group (e.g. a department, team or committee) (Robbins 1997: 105) and to use the group to establish an acceptable level of information security culture. The group's view or pressure could override the individual's moral judgement and mental efficiency/deficiency – referred to as groupthink (Robbins 2001: 9). Pearl Harbour and even the Challenger space shuttle disaster have been linked to groupthink symptoms (Robbins 2001: 9). Strong leadership is required to guide groups in making the right decision and to comply with company policies (e.g. not to copy and distribute pirated software).

On the *organisational* tier, formal structures are added. These regulate whether the organisation operates in a centralised or decentralised manner. Other considerations involve for instance whether a wireless network should be introduced for constant access to e-mail and what security measures should be implemented to protect information. The formal structures implemented by the organisation influence employee attitudes and have an impact on their behaviour (Robbins 2001: 325).

Information security behaviour that is sustained over time evolves into an information security culture that is evident in artifacts, as well as in the values and assumptions of employees (C). Artifacts like technology are usually visible in the organisation, for instance public key encryption. Values reflect

the sense of what ought to be, or the beliefs of the individual ("I ought to have privacy when using electronic communication"), while basic assumptions are related to the subconscious and are part of human nature ("My manager's decision counts above mine") (Schein 1985: 15).

The arrow at the bottom of Figure 5.2 points from information security culture towards the information security component categories. This illustrates that the information security culture that is cultivated influences the effectiveness of the information security components. If employees find the information security policy contents difficult to understand or if they consider it not applicable to their business unit, they might refuse to comply with the requirements of the policy. The information security component (policy) implemented is therefore ineffective and employees could introduce intentional or unintentional threats to the environment. This policy must consequently be adjusted and the effect of the change on the organisational level be managed appropriately.

To illustrate the interaction between A, B and C as depicted in Figure 5.2, the following example can be considered. A formal information security sponsor may be appointed on the organisational tier. This appointment may influence employees to realise that it is important to invest time and money in information security. It could promote the value of responsibility from a senior level. Finally the information security culture could manifest itself on the artifact level – for example, the information security sponsor would be an executive employee who is included in board committee meetings.

5.2.2.3 Level 3 – Information Security Culture Framework

Figure 5.3 (level 3) depicts the ISCF that influences information security behaviour and cultivates information security culture. On the left-hand side, seven categories of information security components are listed as defined in Chapter 4. Each category comprises a number of information security components. An information security component is classified on the organisational, group or individual tier with regard to its influence on

information security behaviour. This classification is based on the main purpose of a component and where it predominantly influences a behaviour tier. It is important to note that components could also influence more than one tier or move between tiers, depending on the maturity of the component and the type and operation of an organisation.

The information security components are classified as follows:

- Components that influence the organisational tier: sponsorship; strategy; governance; risk management; return on investment (ROI); legal and regulatory; policies, procedures; standards; guidelines; certification; best practice; change management. These components have an effect on how the organisation operates and manages information security. Although each of these components in some way or other affect groups and individuals in the organisation, they firstly serve to lay the foundation for defining how information security should be managed in the organisation. For instance, the strategy for information security will be based on the organisational strategy and risks identified in the environment. Again these components reside on an organisational tier, aiding to add formal structures and management for information security in the organisation. In many ways the components categorised on this tier can be seen as the foundation for providing direction to groups of people and individuals in the organisation in terms of protecting information.

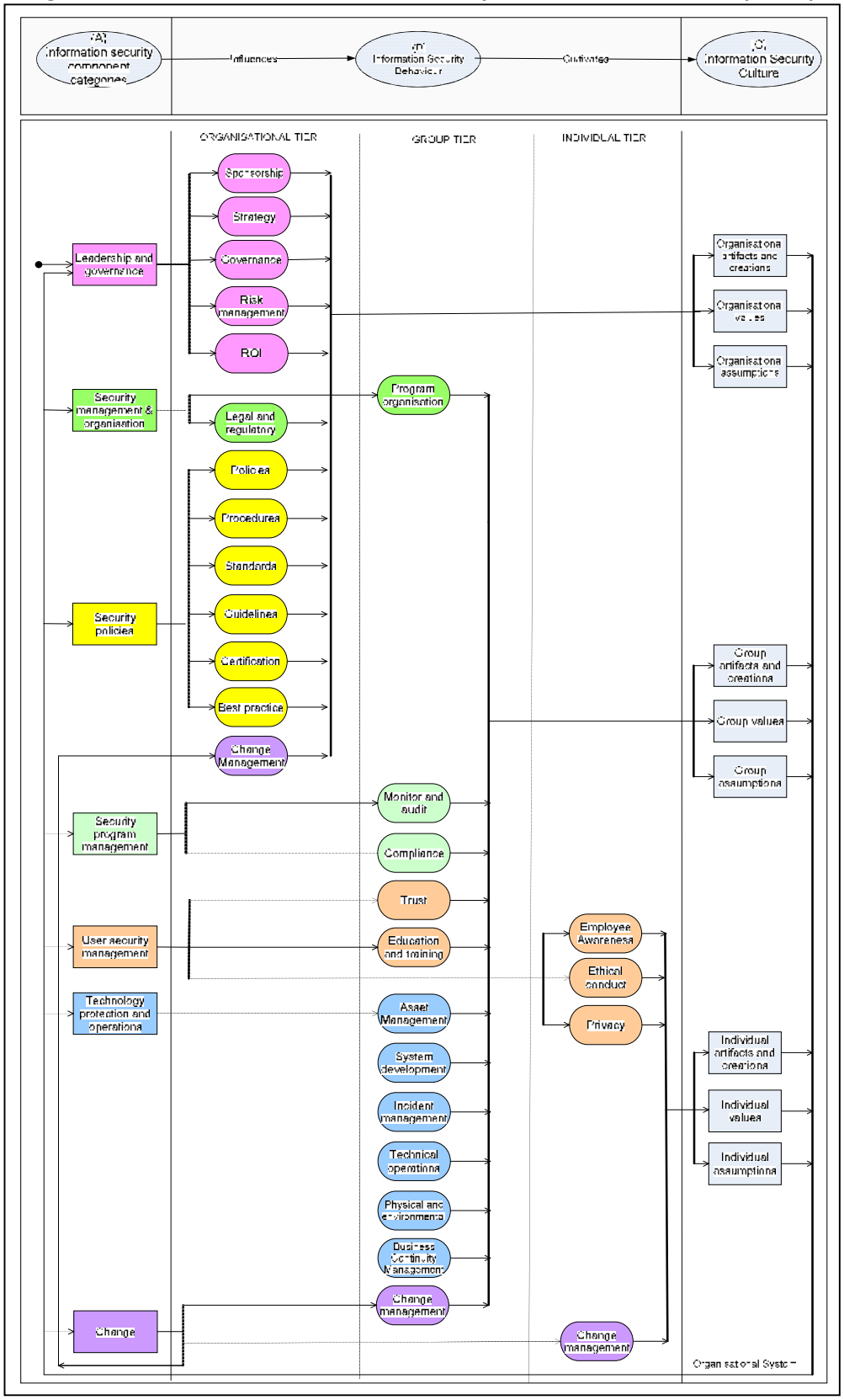
- Components that influence the group tier: program organisation; monitoring and audit; compliance; trust; education and training; asset management; system development; incident management; technical operations; physical and environmental; business continuity management; change management. The components categorised on the group tier mainly influence people as a group in the organisation. For example, education and training are usually provided to employees in a group. Trust can relate to the trust that specific groups, departments or job levels have in terms of management protecting for instance personal information. Assets would need to be secured by departments. System development is

conducted as part of a project consisting of team members or even different parties in the organisation and more than one user would be affected by system changes. All employees in the organisation need to follow the incident management process and a team of individuals could be responsible for the incident management and resolution process. Similarly, technical operations and controls would be deployed to all applications and environments, affecting more than one person.

- Components that influence the individual tier: employee awareness; ethical conduct; privacy; change management. As mentioned earlier, the components can move between tiers and differ from one organisation to the next. For instance, depending on the information security strategy, employee awareness might be conducted on a group tier as opposed to an individual tier due to huge staff numbers and cost constraints. It might not even be conducted at all. However, employee awareness is categorised on the individual tier as the individual is accountable for his/her behaviour and compliance to the information security policy and requirements. Ethical conduct and privacy perceptions are seen as attributes of individuals which could vary between individuals and affect the manner in which they protect information assets.

Change management is categorised on the organisational, group and individual tier as any component that is implemented or changed on any of the tiers would result in change that needs to be managed appropriately.

Figure 5.3 Level 3: Information Security Culture Framework (ISCF)



As indicated above, an information security culture is cultivated on each of the three tiers of information security behaviour. It is reflected in artifacts and

creations, values and assumptions. For instance, an information security policy (policy component) is compiled on an organisational tier and gives direction to both management and employees regarding the protection of information assets. On a group tier, employees work together to implement the policy (program organisation component), while on an individual tier employees are required to change their passwords every 30 days (employee awareness component). One of the outputs of a sound information security culture is strong password usage.

To summarise, an information security culture in the form of artifacts, values and assumptions develops for each component on each of the three information security behaviour tiers. On the organisational tier, information security policy training sessions can be identified as an artifact that has resulted from the policy component. Values such as “I believe the information security policy is applicable to my daily duties” are gradually adopted. Employees visibly exhibit these values through compliance with policies or through management leading by example (mandating and maintaining a clean desk policy). Employees adopt basic assumptions such as “all employees comply with the information security policy” or, “if confidential information must be protected, I must save files in a secure location on the server”.

5. 3 APPLYING THE INFORMATION SECURITY CULTURE FRAMEWORK

Consider this example: Company ABC makes the strategic decision to ensure efficiency in its working procedure. As a result, the decision is taken to equip employees with state-of-the-art technology (strategic component). A risk assessment (risk management component) is conducted to identify security risks and to identify the appropriate controls that are necessary to mitigate the identified risks. The Information Security Officer (ISO) updates the information security policy and compiles procedures and standards to implement the technology (policy, procedure and standard component) on the organisational

tier. Best practice research (best practice component) is considered part of the process of compiling the policies and related documentation.

On the group tier, it is agreed that USB flash disks, Personal Digital Assistants (PDAs) and wireless network access should be deployed to all employees (technology protection and operations component). The current network infrastructure is upgraded by the IT department and procedures are defined for ongoing maintenance (program organisation). Monitoring and audit programs are updated to include monitoring of security risks (monitoring and audit component).

As a result of the above changes, the Help Desk employees might require training in the new technology to assist users with queries. Users also require proper guidance to use the new technology effectively (education and training component). They attend training and must sign off agreement to the updates in the information security policy. Implementing the required controls and processes to support such agreement illustrates a commitment to information security. It helps to establish trust among employees and management, as well as among board members and finally the organisation and its clients (trust component).

On the individual tier, users interact directly with the wireless network and mobile devices. As such, they need to be aware of the information security policy requirements and of potential security risks (awareness component). They must ensure that they have only one connection at a time, make use of strong passwords and see that Bluetooth-enabled devices such as PDAs are set to “non detectable”.

The example of Company ABC taking the strategic decision to ensure efficiency in its working procedure illustrates that the implementation of one component (strategy) affects various components on the three behavioural tiers. The information security culture that develops is evident in the artifacts, values and assumptions.

On the organisational level the introduction of artifacts can be observed, for instance in technology (in this case PDAs or USB tokens). A value that develops on the organisational level could be that the organisation sees itself as dynamic, innovative and moving with the latest technology trends. Its decision about wireless access could result from a belief that sales and profits would be improved through better customer service in more remote locations. Such a belief would be reflected on an organisational level.

On the group level, web-based training (an artifact) can be used to train employees. The value that could be established involves seeing people as an important part of enabling technology and using technology to the benefit of the organisation. An assumption could furthermore be made (also on the group level) that it is “okay to work from home” as the necessary security controls are in place and the IT department monitors and maintains the technology.

Back to the individual tier, employees could make use of e-mail as their main communication method as they have wireless network access and might not all be in the same physical location. A reduction in face-to-face meetings and conversations might be observed and more telephone conferences and e-mail discussions could take place. Employees can also work more efficiently and have immediate access to e-mail messages and the Internet. The introduction of all these artifacts would promote the value of efficiency in the workplace. The assumption could be made that work is done on an individual basis and not in teams, as employees are dispersed geographically, though connected to a wireless network. A change management programme would be designed for all three tiers to assist employees with the transition and to accept the new working procedures.

5. 4 BENEFITS OF THE INFORMATION SECURITY CULTURE FRAMEWORK

The ISCF can assist management in implementing the required information security components that are targeted at the appropriate tiers of employee behaviour. This is achieved by providing management with a comprehensive and holistic view of all the components to consider. It also helps management to understand who in the organisation will be influenced by a specific component and what the effect might be. Furthermore, it aids management in understanding that the implementation of one component potentially has an effect on more than one component and behavioural tier. This will aid management in managing changes effectively and to focus components on the correct tier to bring about the required change to inculcate the acceptable level of information security culture. This could aid in administering an acceptable level of information security and in establishing a culture that would ultimately minimise the inside risk that employees pose to information assets. The framework can be used as a reference to understand how the interaction between employee behaviour and information security components develops in the information security culture of the organisation.

Finally, the ISCF serves as the basis for developing a measuring instrument for assessing the information security culture in an organisation. This framework enables such an instrument to conform to content validity requirements, because it serves as a comprehensive framework for defining the items that are to assess information security culture (Brewerton & Millward 2001). The concept of validity implies that the researcher must ensure that the questionnaire assesses what it claims to assess, namely information security culture (Berry & Houston 1993; Dillon, Madden & Firtle 1993; Furnham & Gunter 1993). An information security culture measuring instrument may help to determine whether the level of the information security culture is enhancing the security of information assets. The metrics derived could provide a roadmap to positively influence developmental areas concerning the information security culture in the organisation.

5. 5 CONCLUSION

Chapter 5 defined the information security culture framework (ISCF) that incorporates the components of the CISF, the influence of the components on the three levels of organisational behaviour and the outputs in terms of information security culture. The interaction between the information security components, organisational behaviour and organisational culture is illustrated in the framework. This framework can be used by organisations to guide the cultivation of an information security culture by considering all the defined components on the different levels in the organisation. The framework can also be utilised to provide a theoretical base to develop an information security culture assessment instrument with which to ensure content validity.

Once the organisation has implemented the ISCF, it can assess the effectiveness of such implementation and whether the information security culture has been enhanced to an acceptable level. Chapter 6 defines a process for assessing the information security culture in an organisation.

PART III

CHAPTER 6

A process for Assessing Information Security Culture

6.1 INTRODUCTION

The current chapter focuses on the development of a process to assess information security culture, ISCULA. Herewith research question 4 is addressed, namely to define how to conduct an assessment of information security culture. Chapter 6 aims to develop practical steps that organisations can use as guidance when conducting an information security culture assessment. An information security culture questionnaire is used as the assessment instrument to assess whether the level of information security is conducive to the protection of information assets. In order to derive valid and reliable data on which management decisions can be based, a statistically sound questionnaire must be used. This questionnaire should conform to validity and reliability requirements. Validity and reliability are therefore incorporated as part of the process to assess information security culture so that the reader may understand its relevance to this research. This contributes in addressing the last research question, namely to provide valid and reliable results when assessing information security culture.

The benefits are discussed of conducting an information security culture assessment on the basis of a survey approach. This is followed by a detailed discussion of the steps involved in the process of assessing information security culture.

6.2 ASSESSING THE INFORMATION SECURITY CULTURE IN AN ORGANISATION

Organisations can assess their particular information security culture by means of questionnaire and survey measures. Questionnaires and surveys are some of the most widely used research tools within the social sciences (Brewerton & Millward 2002: 99). The method is specifically attractive as it

costs relatively little and a potentially large sample of users can participate with minimal resource requirements (Brewerton & Millward 2002: 99). It is traditionally used to measure behavioural content pertaining to attitude and opinions (Berry & Houston 1993: 61) by systematically gathering data from the members of an organisation for a specific purpose (Kraut 1996). To assess the information security culture in an organisation, the attitude and opinions of users regarding information security need to be determined (Martins 2002: 111). Through such an analysis the organisation can assess employees' perception of information security and identify aspects that require attention in order to improve the information security culture to an acceptable level and so protect information assets.

Other alternatives that could be considered are telephone-based surveys or individual surveys whereby an interviewer asks the individual questions and documents the answer. Methods that could also apply are focus groups or assessment centres (Berry & Houston 1993). However, for the purpose of this research study, the method of electronic and/or paper-based surveys is used. The decision arises from cost constraints and provides the opportunity to obtain a larger sample of data to perform the statistical analysis required for validating the assessment instrument.

The paragraphs that follow discuss the benefits of conducting an information security culture assessment by using questionnaire and survey measures.

6.2.1 Benefits of questionnaire and survey measures

Conducting an information security culture assessment (survey) can result in many benefits for the organisation. Some of the benefits that are derived when an assessment is conducted by means of survey measures are listed below and explained in terms of an information security culture assessment.

- *Areas of concern are identified*: A survey manages to determine specific areas of concern among a particular group of people or with regard to a specific topic (Kraut 1996: 5-8). Management might wish to determine

whether Information Technology (IT) staff find the information security policy easier to understand than do Human Resources (HR) staff, or whether the problem is actually that the policy is not communicated effectively to employees.

- *The impact of change is monitored*: Reactions to changes in an organisation can be monitored by means of a survey (Kraut 1996: 5-8). Management may use survey results to determine whether its information security awareness programme has had the desired or expected effect. When departmental training sessions are conducted to explain information security requirements, management can easily detect that these have been effective when the survey results of the topics covered in the training sessions improve significantly from one assessment session to the next.
- *Input is provided into management decisions*: The information obtained through an information security culture survey may influence future decisions by management (Kraut 1996: 5-8) and serve to identify areas that require change or improvement (Church & Waclawski 1998: 12). For example, the survey may uncover that employees of a specific job level prefer television broadcasts of information security messages, whereas incumbents on another job level prefer group discussions. The awareness programme can therefore be focused and tailored on the basis of key findings identified in the assessment. Assessment results can furthermore provide some motivation for the awareness programme and even for information security budget purposes. This will affect the prioritisation of funds and awareness initiatives.
- *An additional communication channel is established*: The survey in itself is a way of raising awareness with regard to information security. It also provides a two-way channel of communication by reporting feedback on survey results to employees (Kraut 1996: 5-8). Assessment results can also be communicated to the Board as part of information technology (IT) governance initiatives.
- *Meaningful results are yielded*: The results of psychometric instruments are meaningful and powerful due to the statistical robustness that has allowed the researcher to draw conclusions and make predictions based on the obtained data (Brewerton & Millward 2002: 94). The researcher can

conclude whether there is a lack of leadership and, should it improve, whether the impact will have a positive influence on the information security culture.

- *Survey data can be compared*: Comparability is possible with the use of psychometric instruments that have been normed and standardised, following rigorous validity and reliability testing (Brewerton & Millward 2002: 95). Various comparisons can be made with regard to data of different departments, job levels, geographical areas or even people who attended information security induction training compared to those who did not. This allows the researcher to focus future efforts and even benchmark them against a future survey's data to analyse the impact of changes.
- *Costs are relatively low*: By using a computerised approach to distribute and collect the survey responses, administration and analysis are speeded up and the cost of the assessment is reduced – compared to the use of focus groups and interviews (Brewerton & Millward 2002: 95).

6.3 BACKGROUND ON PROCESSES TO ASSESS INFORMATION SECURITY CULTURE

Two research perspectives, namely those of Schlienger and Teufel (2005) and Martins and Eloff (2002), focus on the assessment of information security culture and describe a process that can be used to assess information security culture in an organisation. The next paragraphs provide a high-level overview of the processes proposed and conclude with a motivation for the process as proposed in this research study.

6.3.1 Schlienger and Teufel

In their research, Schlienger and Teufel (2003, 2005) describe a process for conducting an information security culture assessment in an organisation. The processes consists of four steps, namely diagnosis, planning, implementation and evaluation.

The *diagnosis* phase sets off with a pre-evaluation of the information security culture in the organisation. An analysis is conducted of information security documentation, such as the organisation's information security policy, a questionnaire to employees, interviews with security officers, and observation exercises (verification of a clear-desk policy).

In the second step, *planning*, the target or objective for the development of an information security culture is defined. The market segments are defined, for example managers, operational and IT staff, thus enabling the researcher to segment the data for comparison purposes.

The third phase, *implementation*, incorporates aspects of internal marketing, human resources management and organisational development (Schlienger & Teufel 2003a). The researchers argue that internal communication, management buy-in and an awareness and training programme are key elements in initiating an information security culture change and maintaining the targeted information security culture. Implementation should take place within the context of defined activities, responsibilities, resources, schedules and the budget (Schlienger & Teufel 2005).

The implementation step is followed by *evaluation,* which provides insight into how efficient and effective the implemented actions have been.

This approach comprehensively aids the organisation to assess its information security culture and to address the areas identified for development by the assessment. It is structured and practical and can be used to guide the management of an organisation, as they are required to conduct an information security culture assessment and follow up their findings with action plans.

6.3.2 Martins and Eloff

Martins and Eloff also propose an assessment process consisting of four steps – develop the questionnaire, conduct the survey process, analyse the

data and interpret the survey data. The first step outlines how to compile an information security culture questionnaire by considering the objective of the questionnaire and key considerations in drafting the individual questions (for instance, not using jargon).

The survey process entails the steps used to determine the sample population, the distribution and collection of the questionnaires and the completion of the survey. The third step refers to the statistical analysis of the survey results and the last step to the interpretation of results so as to make recommendations. The latter are intended to address the areas for development, as identified.

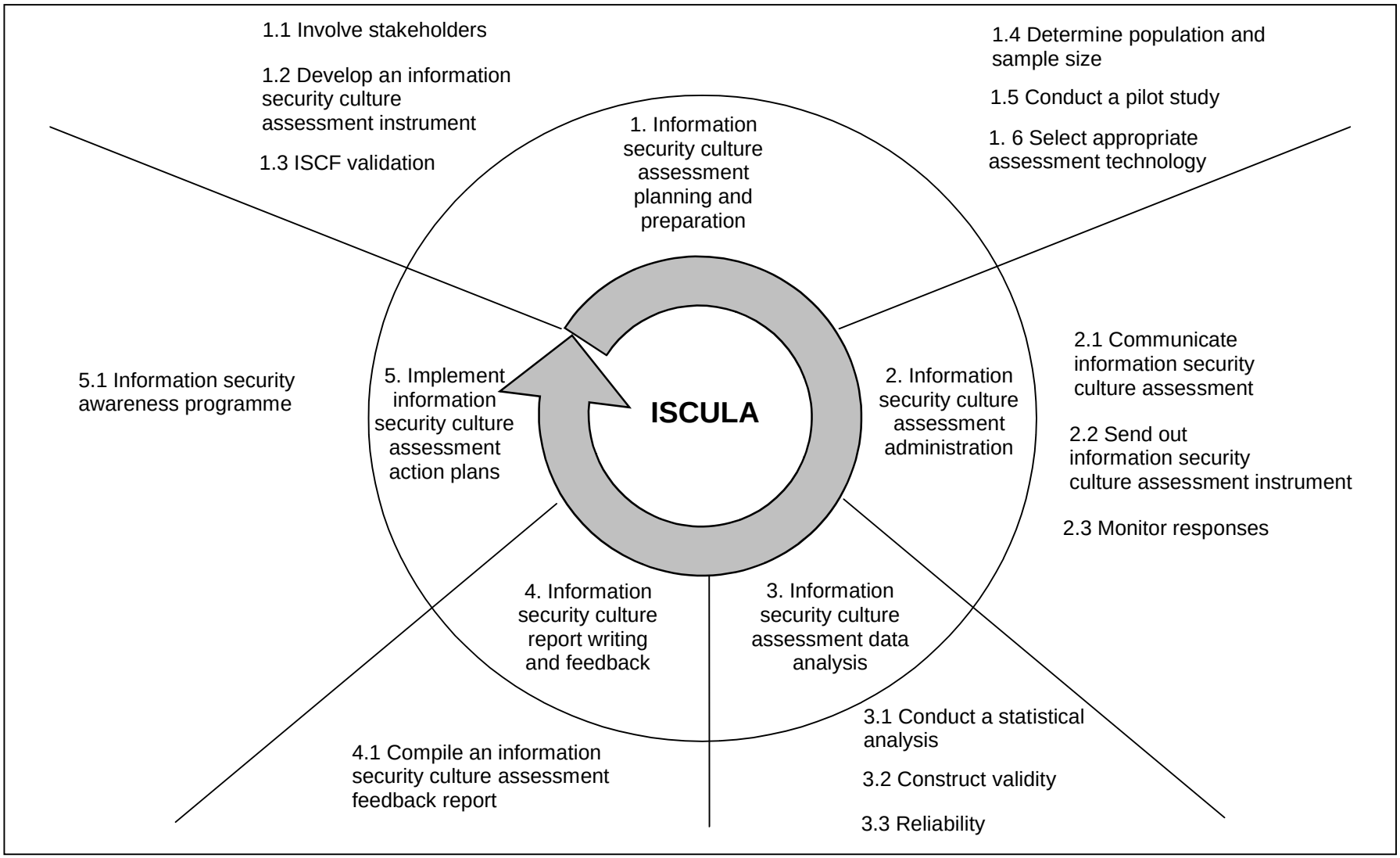
The survey process proposed by Martins and Eloff focuses on the researchers' perspective to conduct an assessment of information security culture and not specifically of the organisation. However, management could still use the process as guidance when conducting an information security culture assessment.

The available processes for conducting an information security culture assessment do not provide detailed steps describing how to ensure the validity and reliability of the questionnaire that is used. However, such steps could be incorporated under the preparation of the questionnaire and the statistical analysis of its results. It would aid the organisation if the process were to describe steps for ensuring a statistically sound measuring instrument. This would make it possible to ensure that the organisation is in actual fact measuring information security culture and not concepts relating to it, which could skew the results and lead to inaccurate management decisions. Researchers as well as organisations would benefit from a process that combines the practical implementation steps of Schlienger and Teufel and the research perspective of Martins and Eloff.

6.4 PROPOSED PROCESS TO ASSESS INFORMATION SECURITY CULTURE

Different steps may be followed to conduct a survey and, as such, an information security culture assessment. According to Kraut (1996) the process of designing, implementing, administering and reporting back on survey data is key to the success of the survey and perhaps even more important than the actual results generated. Figure 6.1 portrays a proposed 5-step process, “Information Security Culture Assessment” (ISCULA) to assess information security culture. It is constructed by incorporating steps considered by Berry and Houston (1993), Kraut (1996), and Brewerton & Millward (2002) and outlines the five main steps for conducting an information security culture assessment (survey) in an organisation using a questionnaire (assessment instrument). This process can assist management in conducting the information security culture assessment by providing structure and guidance for the process to follow. It also contributes by planning the information security culture assessment, assigning roles to employees to conduct the different steps, contributing to the quality of the data obtained and identifying action plans.

Figure 6.1 Process for assessing information security culture (Information Security Culture Assessment - ISCULA)



The following paragraphs discuss each step of the process whereby information security culture can be assessed.

6.4.1 Step 1: Information security culture assessment planning and preparation

The first step in conducting a survey is to plan it (Berry & Houston 1993: 64). The planning and preparation phase of the information security culture methodology consists of seven steps, as proposed and discussed below.

6.4.1.1 Step 1.1: Involve stakeholders

The project must be initiated by means of a formal project introduction meeting to obtain buy-in from relevant stakeholders and to discuss the project plan of operations (Berry & Houston 1993:65). Typical stakeholders in respect of the information security culture survey would be the Information Security Officer, the Information Security Awareness team, the Risk Manager, the Human Resources representative, the Internal Audit representative, Communication and Marketing representatives, the Information Technology representative and a union representative. These different representatives are required, as the conducting of the information security culture survey will potentially require interaction from each of these representatives to ensure the efficiency of the project. For instance, the Information Security Officer owns the project and his awareness team will eventually use the results of the survey as input into the awareness programme to address areas for development. The Risk Manager is involved from a risk perspective, as internal employee behaviour is one of the threats to information assets that must be addressed. Internal Audit might use the survey results as part of their information security audit. The Communication and Marketing representatives are required to assist with communicating the survey to the target population and will know from experience what method of communication is the most effective in the organisation. The Information Technology representative needs to configure the technology for distributing the questionnaire electronically.

6.4.1.2 Step 1.2: Develop an information security culture assessment instrument

The questionnaire to be used in the assessment has to meet the objectives of the assessment and must be effective in identifying issues relating to the subject matter being assessed, namely information security culture. If the researcher uses a pre-developed questionnaire, the questions must be customised (Berry & Houston 1993) to suit the organisation's environment. This can be achieved by conducting a workshop with all stakeholders. Care must be taken to ensure that technology staff as well as business representatives attend the workshop. This will ensure that the questionnaire is not merely technology specific, but that business-orientated employees will also understand the questions and terminology.

One of the aspects that are customised is the organisation-specific terminology that is incorporated in the questionnaire statements, for instance the use of the concept *team leaders* instead of *managers.* A questionnaire usually contains biographical questions that are used to understand the composition of the population who will answer the questionnaire and also to segment the data for analysis. The biographical questions should thus be adapted to reflect the selected target population. These questions generally cover business areas, geographical areas, length of service and job levels in the organisation.

Church and Waclawski (1998: 54) recommend that if a questionnaire has not been developed yet, the researcher has to gather preliminary information about important issues regarding the subject matter to assess. For instance, what components should be considered when assessing information security culture? An information security culture framework (ISCF) can be used as the foundation to identify the components of information security culture and to phase the statements. Interviews or group discussions can furthermore be used to identify key issues and give the researcher an idea of which questions to ask (Walters 1996: 68) in the specific organisational environment (e.g. managers believe employees do not know where to obtain a copy of the

information security policy or no one is motivated to attend the information security induction training presentation). The initial questionnaire can be drafted based on the identified information security components (e.g. components in the ISCF) and issues identified in the organisation and relating to information security culture.

The statements designed to assess information security culture can be referred to as the information security culture statements. Issues identified in the focus group discussions might differ from the information security culture statements that are based on the ISCF. These questions or statements can be included in a separate section in the questionnaire so as not to influence the validity of the information security culture statements.

6.4.1.3 Step 1.3: ISCF validation

Validity is a complicated statistical term, but necessary to consider in order to construct a powerful survey instrument (Furnham & Gunter 1993: 45). The concept of validity implies that care must be taken to ensure that the questionnaire assesses what it claims to assess (Berry & Houston 1993: 299-300; Dillon, Madden & Furtle 1993: 294; Furnham & Gunter 1993: 45). A valid questionnaire consistently yields reliable and stable results over time (Dillon, Madden & Furtle 1993: 294). Reliability can be achieved without validity (Huysamen 1988: 33). In other words, although results of a measurement can be reproduced and be consistent, the questions that are asked may be about irrelevant factors. The opposite is true for validity, where a measurement that is unreliable can never be valid. Huysamen (1988: 33) explains validity by using the example of determining the length of students to indicate their academic success. It would be easy to find an accurate measuring tape to measure each student's length, thus providing reliable length measurements. These measurements are, however, not valid in determining academic success. The information security culture questionnaire must therefore focus on what constitutes information security in an organisation and the user's perception thereof to correctly determine the information security culture in the organisation. Questions or statements that are not relevant to information

security culture, for instance, “The bonuses of information security staff correspond to the bonuses of employees at competitors”, affect the validity of the questionnaire and should be avoided.

Content validity evaluates the theoretical perspective(s) that drive the measuring instrument and the way in which the theory has been used to develop the items that are measured for information security culture (Brewerton & Millward 2001: 90; Furnham & Gunter 1993: 45). In the case of the information security culture questionnaire, and for the purpose of this research study, content validity is ensured by considering the components of the ISCF to structure the questionnaire statements. If an existing questionnaire is used, content validity has to be determined by mapping the information security culture questionnaire that is used against the ISCF and determining the adequacy of coverage for each subject area. In other words, each component of the ISCF must be covered by a statement or question in the questionnaire to ensure that the results obtained from the assessment are valid and can be used by management to make business decisions. This applies both to designing a questionnaire from anew and to mapping an existing questionnaire to the ISCF.

Table 6.1 is provided to illustrate how an existing information security culture questionnaire’s content validity can be determined. The component category of “Leadership and governance” is used with the “Sponsorship” component as defined in the ISCF. The third column lists statements of an existing information security culture questionnaire that could possibly be mapped to the sponsorship component. The (in)adequacy of the statements covering the component is indicated in the fourth column (“Adequate”), based on whether the statements relate to the meaning and objective of the component as intended with the ISCF. The last column lists proposed statements when the existing statements are not adequate to assess the component. These statements can be used in their stead to ensure that content validity is met for the specific component. For example, the statement in the existing questionnaire, namely, “I think it is important to implement information security in the organisation”, does not assess specifically whether members of senior

management believe the implementation of information security to be important. The statement is, however, supposed to assess this concept, as the component "sponsorship" focuses on senior management's commitment in the organisation. It is consequently replaced by the proposed new statement that focuses on senior management and that conforms to the definition and objective of the component as defined in Chapters 4 and 5.

Table 6.1 Content validity analysis of an existing questionnaire

Component category	Components	Existing information security culture questionnaire	Adequate	Proposed information security culture statements
Leadership and governance	**Sponsorship**	I think it is important to implement information security in the organisation.	No	Senior management in ABC is committed to the protection of information. Management perceives information security as important to protect information.
	Strategy	The organisation has an information security plan.	No	I believe it is necessary to protect information to achieve the business strategy of ABC. I believe ABC pays adequate attention to an information security strategy in order to protect information. The information security controls implemented by ABC supports the business strategy.

The response rate, answers of respondents, capturing of data and statistical analysis are affected by the way in which questions are structured in a questionnaire. Various researchers (Dillon, Madden & Firtle 1993; Church & Waclawski 1998) have established principles that must be considered when designing questions that will provide valid and reliable data.

The next section briefly outlines the principles to be taken into account when designing a questionnaire's statements and/or questions.

a. Brevity and clarity

Statements formulated for the questionnaire must be brief, clear, concise and to the point (Dillon, Madden & Firtle 1993: 304; Church & Waclawski 1998: 80). A statement should be phrased as follows: *"The organisation has a documented information security policy"*, rather than *"The organisation has information security requirements that I must comply with and that are stated in a policy where information security is seen as an important aspect",* which is not only longer, but could also be unclear.

b. Respondent's language ability and specialised knowledge

The respondents' language ability should be taken into account in the phrasing of statements. The researcher needs to make sure that the words are not too difficult to understand or do not involve complex issues or require specialised knowledge (Brewerton & Millward 2002: 104; Kraut 1996: 163). Say: *"The business continuity plan explains what each person must do in the event of a disaster",* rather than: *"The organisation has a business continuity plan that includes procedures for the IT department to merge master file data into predisaster files".*

Many phrases or terminology in the information security field are specialised knowledge that employees in general might not be familiar with. Terms such as threats, information assets, business continuity plan, information security incident, best practice guidelines and even information security must be defined upfront in the questionnaire to prevent confusion and misinterpretation of the statements. To clarify terminology further, practical examples can be provided in some statements or questions. For instance, to clarify what is intended by information security *requirements,* the following can be added: "e.g. what Internet usage is allowed and how to make backups". It is imperative that the examples provided in all statements must be evaluated

and revised when the questionnaire is customised for a particular organisation. Each organisation is different and applies information technology and implement information security controls differently. One organisation might expect employees to use digital certificates while another insists on passwords. The examples provided in statements must therefore be tailored to each organisation's environment.

c. Short sentences free of jargon

Consider making use of short sentences that are free of jargon when constructing statements (Brewerton & Millward 2002: 104, Kraut 1996: 163). Constructing statements that use terms, abbreviations or expressions that are familiar only to information security professionals or IT employees could be confusing to other employees, for instance in the financial or sales department.

For example: *"The SDLC process documented in the ITS policy includes security considerations for IT employees that must be followed in small, medium and large system developments, whether internally or by an external consultant".* Employees who do not work in the information processing department might not know that SDLC stands for System Development Life Cycle, nor that ITS stands for the Information Technology & Security policy. The statement should rather be structured as follows:

Which of the following do you agree with? (Select where appropriate)
There is a software development policy (SDLC) in the organisation. [Yes/No]
The internal software developers must comply with the above policy. [Yes/No]
Contracting software developers must comply with the above policy. [Yes/No]

d. One concept, issue or problem

Questions or statements should measure only *one* concept, issue or problem. The researcher should ensure that statements do not include two opinions that are joined together (double-barrelled questions) (Brewerton & Millward

2001: 104; Church & Waclawski 1998: 79-80). Statements that could have more than one meaning should be avoided (Kraut 1996: 163, Walters 1996: 109).

Statements such as: *"I know what an information security incident is and know where to report it"* could cause confusion because more than one concept is measured. What does the respondent answer if he/she does not know what an information security incident is, but knows that incidents must be reported to the Helpdesk? Instead, two different questions should be asked:

I know what an information security incident is. [Yes/No]
I know where to report information security incidents. [Yes/No]

e. Clearly diverging response choices

Response choices to each statement should contain explicit alternatives to be considered by the respondent (Dillon, Madden & Firtle 1993). For example:

I am informed about information security requirements through e-mail… (Tick only one)

1. once a month [ ]
2. once or twice a month [ ]
3. two to three times a month [ ]
4. three or more times a month [ ]

If ABC sends out information security awareness e-mail messages twice a month, the respondent will not know whether to select option 2 or option 3. Results could also be affected, as option 2 could be seen as negative and option 3 as positive. Options should rather be constructed as follows:

I am informed about information security requirements through e-mail… (Tick only one)

1. once a month [ ]
2. two to three times a month [ ]

3. four to five times a month [ ]

4. six or more times a month [ ]

f. Proper layout of questionnaire

The layout and format of the questions must be attractive and well presented, as this could enhance the response rate significantly (Brewerton & Millward 2002: 106). The following considerations were taken into account in designing the final information security culture questionnaire as presented in this research:

- Brewerton & Millward (2002: 107) emphasise that a covering letter with instructions is very useful in elevating response rates. It is imperative to ensure that a senior employee signs off the covering letter. A covering letter from the Chief Executive Officer will promote responses much more than a covering letter from the IT Manager.
- Part of the covering letter must focus on the confidentiality of the survey and ensure employees of the anonymity thereof (Brewerton & Millward 2002: 107). Employees might be reluctant to take part in a survey if their answers can be traced back to them.
- The time taken to complete the questionnaire must not exceed 45 minutes, as extremely high motivation will in such a case be required of the respondents to participate in the survey. The questionnaire must also not be shorter than two pages, as a short questionnaire is neither taken seriously nor likely to address any substantive research question (Brewerton & Millward 2002: 107). Church and Waclawski (1998: 62) suggest that a questionnaire should have between 80 and 100 questions, not including the biographical questions.

6.4.1.4 Step 1.4: Determine population and sample size

Various sampling techniques can be deployed to define the sample size of the population, for instance probability sampling, simple random sampling, systematic sampling, stratified sampling, quota sampling or snowball sampling – to mention but a few (Brewerton & Millward 2002: 114-120). It would be

ideal to have the information security culture questionnaire sent to all employees in the organisation to ensure reliability of the data. The questionnaire could also be sent to clusters of employees with similar characteristics, such as business units and geographical areas (Brewerton & Millward 2002: 114-120). Depending on the cost implications and practical considerations, the organisation might decide to only collect information from a subset (sample) of the population. Care must however be taken to ensure that the sample "provides a faithful representation of the total population selected", and "that the sample is reliable" (Brewerton & Millward 2002: 114).

6.4.1.5 Step 1.5: Conduct a pilot study

Before the questionnaire can be rolled out to the target population, it has to be pre-tested on a small sample of employees. This would allow the researcher to understand the anticipated reactions of the large group and to revise or restructure questions where necessary (Berry & Houston 1993:65). A group of approximately 20 employees in the organisation, who represent different characteristic of the target population, must be requested to complete the pilot survey in order to test the face validity of the questionnaire. Face validity is concerned with whether the questionnaire is assessing what it says it does on the "face of it" (Berry & Houston 1993:175). Minor adjustments are usually made to some of the questionnaire statements to ensure that all employees will interpret the questions in the same manner. For instance, examples could be added to some terms and the word "department" could be replaced with the terminology of the organisation, such as "business area". It is imperative that the project owner or even the required stakeholders sign off the final information security culture questionnaire to prevent a cycle of ongoing adjustments to the questionnaire.

6.4.1.6 Step 1.6: Select appropriate assessment technology

A process for distributing, completing and collecting the questionnaires needs to be established. There are numerous ways of collecting data, for instance by paper surveys, e-mail, intranet, telephone and interviews. Various survey tools

are also available and many organisations make use of their own survey software. As each organisation's environment is unique, the process best suited for the organisation must be selected in conjunction with its stakeholders.

6.4.2 Step 2: Information security culture assessment administration

Survey administration is the process used to distribute the questionnaires to the target population and obtain the completed questionnaires back for analysis purposes. Survey administration consists of the three steps discussed below.

6.4.2.1 Step 2.1: Communicate information security culture assessment

Communicating the survey and its objectives to employees is crucial in order to enhance the response rate and quality thereof (Dillon, Madden & Firtle 1993: 166). If questions are of a sensitive nature and employees wish to remain anonymous, the organisation must ensure that individual responses cannot be identified (Berry & Houston 1993: 61). The information security culture questionnaire can be communicated using various methods. These methods must be in line with the input provided by the communication and marketing stakeholders. The organisation could for instance send out an e-mail a week prior to the launch of the survey to notify employees thereof and to explain the objective. Weekly e-mails can then be sent to remind employees to complete the questionnaire before the due date. Other methods such as a competition to motivate responses, posters or incentives can be used.

6.4.2.2 Step 2.2: Send out information security culture assessment instrument

The information security culture questionnaires are distributed in line with the process selected by the organisation – whether electronically or paper-based. The questionnaire may be e-mailed to employees or they could complete it on

the organisation's intranet. Alternatively, employees may complete the questionnaire on the Internet, provided there is adequate security controls in place (for instance a username and password to access the questionnaire).

In instances where employees do not have access to technology, paper copies of the questionnaire can be handed out to employees to complete and return to a manager or they could even mail it to a central location.

6.4.2.3 Step 2.3: Monitor responses

Responses must be tracked to ensure that a statistically representative response is obtained for each biographical area in which the data will be segmented, for instance the various job levels or departments. Various statistical methods can be used to determine the required sample size, for instance the method designed by Krejcie and Daryle (1970: 608-609). For segments in which the responses have been inadequate, trends can be considered and focus groups can be conducted to confirm the results.

6.4.3 Step 3: Information security culture assessment data analysis

The data obtained by means of the information security culture survey is analysed using statistical methods. The possible types of statistical analysis that will be required should be agreed in the planning phase (Brewerton & Millward 2002: 143). Statistical analysis can also be used to further validate the questionnaire.

6.4.3.1 Step 3.1: Conduct a statistical analysis

The following statistical analyses can be considered to identify what items to focus on so as to improve the information security culture in an organisation:

- Frequency distribution: This is the frequency with which a variable occurs, i.e. how often a specific score turns up (Howell 1995: 28-29).

- Mean: The mean is the average score of the results, in other words, the sum of the scores divided by the number of scores (Howell 1995: 51-56).
- Standard deviation: This is a measure of the average of the deviations on each score from the mean. For instance, a standard deviation of 0.787 indicates a deviation of 0.787 units from the mean, whereas a standard deviation of 0.342, which is closer to zero, indicates a much closer deviation to the mean (only 0.342 units), which is more positive (Howell 1995: 67-69).
- T-tests: T-tests are used to determine differences between two groups (Brewerton & Millward 2002: 145). For instance, is there a significant difference between the perception of employees in the Financial Department and employees in the Human Resource Department regarding the clarity of the information security policy?
- Anova tests (analysis of variance): These are used to determine the difference between more than two groups (Brewerton & Millward 2002: 145). The organisation might require insight into how each job level perceives the applicability of the information security policy.
- A cut-off of 64% on the percentages can be used to differentiate between positive areas and areas for development: This percentage gives a reasonable cut-off to distinguish between positive and potentially negative perceptions (Odendaal 1997). The cut-off percentage must be agreed with the stakeholders before the survey is conducted. It could also be argued that a much higher cut-off must be used, as the organisation requires 100% security. Even a single user whose behaviour deviates from the information security policy could introduce a potential risk to the protection of the organisation's information assets.

6.4.3.2 Step 3.2: Construct validity

The validity of a questionnaire can be determined through the statistical analysis of its results. The outcome of such analysis will aid the researcher to improve the questionnaire for future use and to provide statistically valid results.

According to Brewerton and Millward (2002: 92-93) a factor analysis can be employed to assess the robustness of the questionnaire's dimensions, thereby identifying clusters of questions and forming new dimensions. A dimension is a number of questions grouped together that relate to one another, for instance the questions regarding the information security policy are grouped together in a dimension.

The technique of structural equation modelling (SEM) can be used to perform such a statistical analysis. SEM involves the "amalgamation of multiple regression and confirmatory factor analytic techniques to assist in the assessment of developed models" (Brewerton & Millward 2002: 165). Factor analysis is a statistical technique that is employed to determine or uncover any underlying 'structure' that may exist in the data (Brewerton & Millward 2002; Howell 1995). A confirmatory factor analysis is performed to determine whether the predefined factors (dimensions) of the information security culture questionnaire have a high correlation. The objective is to determine whether the dimensions of the information security culture questionnaire can be accepted as determined through various statistical parameters. Should the parameters be within the acceptance criteria, the theoretical model (ISCF components) can be accepted.

To evaluate the fit of the theoretical model (ISCF components) and the empirical data the parameters listed below are considered.

- The Goodness of Fit Index (GFI): GFI identifies whether there is a good fit between the seven theoretically defined factors and the data derived from the survey (Howell 1995: 358). The GFI value should be greater or equal to 0.95 for the theoretical model to be accepted (Brewerton & Millward 2002: 168; Schermelleh-Engel et al. 2003).
- The Adjusted for Goodness of Fit Index (AGFI): AGFI is used as an index to adjust for bias as a result of model complexity. The more complex the model, the lower the index will be. The value criteria for the index should be greater or equal to 0.95 for the theoretical model to be accepted (Brewerton & Millward 2002: 168; Schermelleh-Engel et al. 2003).

- The Root Mean Square Residual (RMR): RMR is a measure of overall badness-of-fit. The closer to 0, the better the model fit (Brewerton & Millward 2002: 168; Schermelleh-Engel et al. 2003).

The results of the above parameters provide the researcher with an indication as to whether the components of ISCF and the manner in which the statements are grouped in the questionnaire are statistically acceptable. Should the parameter criteria be met, they confirm the theoretical model (ISCF) and contribute to the validity of the questionnaire. If the parameter criteria are not met, the questionnaire has to be adapted based on the results of the analysis. Only then can it be reused in another assessment, and a statistical analysis should again be conducted to assess the construct validity.

6.4.3.3 Step 3.3: Reliability

Reliability is concerned with the internal consistency of a proposed or existing scale containing a number of items (Brewerton & Millward 2002: 89; Huysamen 1996: 20). Huysamen (1996: 19-20) explains the concept of reliability by using a stretchable measuring tape to measure the length of people. If the measuring tape is longer on warm days and shorter on cold days, the same person's length will vary if it is measured on different days, despite the fact that the person's length remains consistent.

The purpose of Cronbach's alpha (item analysis) technique is to determine the reliability of an instrument (questionnaire) and the degree to which the items selected (ISCF components) 'fit into' the intended area (information security culture) measured. The reliability figure obtained provides an indication of the level of consistency across the scale items (Brewerton & Millward 2002: 89) and varies between 0 and 1. Cronbach's alpha is used to examine the frequencies and descriptive statistics for each item on the survey across all responses obtained (Church & Waclawski 1998: 172). Items with a coefficient of between 0.6 and 0.7 can be accepted as an absolute minimum to be identified as a factor (Brewerton & Millward 2002: 89; Huysamen 1996: 30). This will help the researcher to use statements that measure information

security culture accurately. Respondents will also interpret the questions in the same manner irrespective of when, where and how the assessment is conducted (Huysamen 1996: 20).

6.4.4 Step 4: Information security culture assessment report writing and feedback

The results and findings of the survey must be summarised in a report. Walters suggests that there should be two reports - one for management and one for employees who participated in the survey (Walters 1996: 140).

6.4.4.1 Step 4.1: Compile an information security culture assessment feedback report

The typical report could be structured to include an executive summary, background to the research, the method and procedure, results, interpretation of results and finally recommendations (Brewerton & Millward 2002: 179-180). The executive summary is valuable as it highlights the practical significance of the findings that are of most interest to the organisation (Brewerton & Millward 2002: 177-178). Brewerton and Millward suggest that the executive summary comprises the following:

- What was done?
- How was it done?
- When was it done?
- Who and how many respondents were involved?
- What was found?
- What are the implications of what was found?
- What is recommended?

The findings of the information security culture assessment can be presented to management in the format of a presentation. Visual support such as overheads, flip-charts, examples, slides and handout material can be used for this purpose (Brewerton & Millward 2002: 182). Findings could also be posted

on the organisation's Intranet or a summary can be e-mailed to employees to provide feedback.

6.4.5 Step 5: Implement information security culture assessment action plans

After completing the survey it is important to follow through with action plans to ensure that the survey exercise was worthwhile (Walters 1996: 154). Resistance may well be encountered as change is traumatic and "organisations are notoriously resistant to it" (Walters 1996: 156). Walter also (1996: 157) suggests that before the survey is launched, everyone involved must understand the implications of the survey and what the specific impact of the findings might be. Such a timely discussion with management will also prepare them for a possibly unfavourable outcome. According to Walters the next step would be to ensure that all the people involved stay informed throughout the course of the survey and that positive commitment is obtained from senior management (Walters 1996: 160). This can typically be structured through a workshop where commitment to the final information security culture assessment findings is obtained and tasks are allocated to action people.

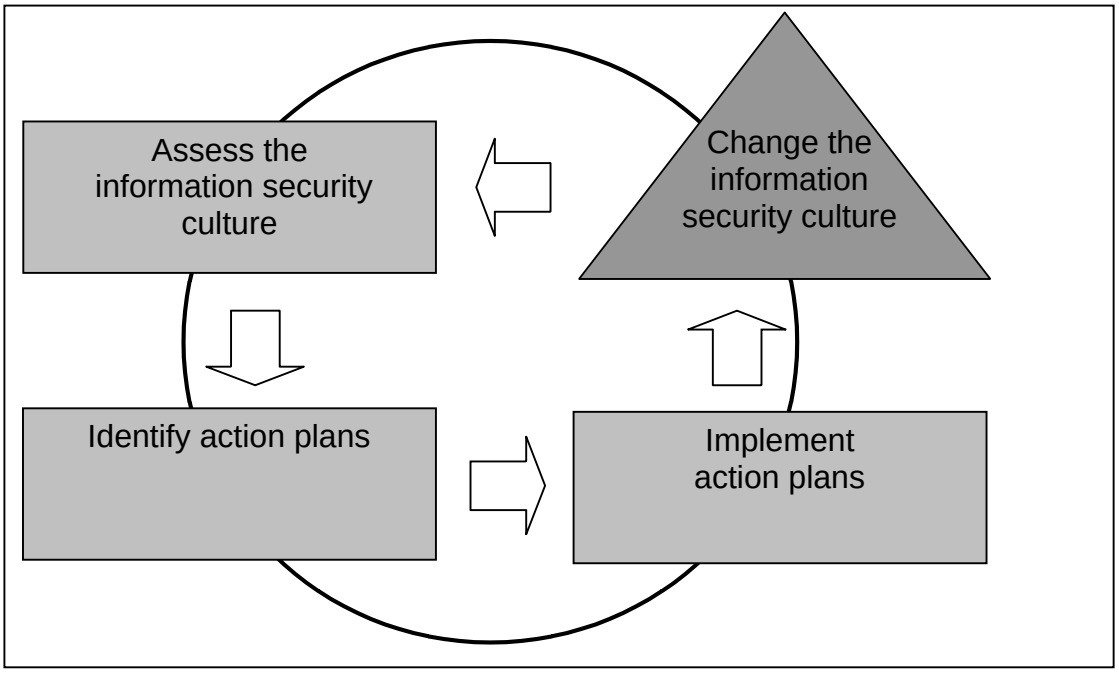
6.4.5.1 Step 5.1: Information security awareness programme

One way of addressing the findings that emerge from the information security culture assessment is by implementing an information security culture awareness programme. This is because such programmes are seen as a stepping stone towards developing an information security culture (Grant 2005; Helle 2005; Helokunnas & Ilvonen 2004; Purser 2004; Starnes 2006; Steward 2006; Thomson 2004). Figure 6.2 illustrates the steps that could be followed to implement the information security culture findings.

The process starts with an assessment of the organisation's information security culture. As output, action plans for developing specific areas are identified. These could be to communicate information security concepts to employees, to explain the information security policy or to provide training of

employees for specific job levels so as to take responsibility for information security in the organisation. A list of action plans is thus compiled. Individuals are assigned to the actions and due dates are agreed on. The action plans could be incorporated into the organisation's communication plan or into its information security awareness programme. Due to the actions identified, the current information security awareness programme, induction training and communication material might need to be revised. These revisions may also be addressed within the context of the information security awareness programme. The actions may then be implemented and progress needs to be monitored. Over time, changes will start to emerge as employees' understanding of their roles towards information security improves, new recruits are trained efficiently to protect information assets and effective communication methods are used to convey information security messages. Over time, the information security culture will also start to change. To determine whether the action plans were indeed effective and had the desired effect on the information security culture, a second information security culture assessment is conducted. The results of the first and second assessment can then be compared for further insight. New action plans can again be identified and the cycle will continue.

Figure 6.2 Information security culture change cycle



6.5 CONCLUSION

The objective of Chapter 6 was to define a process for conducting an information security culture assessment in an organisation in order to address research question 4 and 5. The survey approach was selected as it is effective in measuring behaviour, attitudes and the perceptions of employees – thus the information security culture. The proposed process for assessing information security culture proves to be of a cyclical nature and consists of various steps. An information security culture questionnaire constitutes the heart of the process as it serves as the instrument for assessing employee perceptions and opinions about information security in the organisation. The data derived from the assessment provides the organisation with an indication of the level of information security culture in the organisation and whether there are areas for improvement.

Chapter 7 discusses an empirical study that will illustrate the practical implementation of the process described in this chapter.

CHAPTER 7

An Empirical Study

7.1 INTRODUCTION

In this chapter an empirical study is presented of an information security culture assessment. The objective is to derive data that can be used to validate the information security culture assessment instrument (questionnaire) used in the assessment, thereby providing a valid and reliable tool that can be used by organisations to assess the in-house level of information security culture. Chapter 7 therefore contributes to address the fifth research question illustrating how to provide valid and reliable results when assessing information security culture.

7.2 BACKGROUND

As previously discussed, a valid and reliable assessment instrument must be used to assess the information security culture in an organisation. In order to design such an assessment instrument, data is required from a survey in which the information security culture assessment instrument was tried out, in order to perform a statistical analysis. In the current study, the researcher performed an information security culture assessment in an organisation as part of a empirical study aimed at validating the proposed information security culture assessment instrument.

The Information Security Culture Assessment process (ISCULA) proposed in Chapter 6 is applied to assess the information security culture in the organisation. In the sections that follow the empirical study is discussed.

7.3 INFORMATION ON EMPIRICAL STUDY ORGANISATION

7.3.1 Background to organisation used for empirical study

The empirical study was conducted in a South African member firm of an international firm that performs audit and advisory assignments. The organisation employs approximately 3 000 employees in South Africa. The Information Security Function (ISF) is integrated within the organisation's business operations and is considered mature by the organisation. There is a dedicated Information Security Officer (ISO) with a team of six people to ensure that information security controls are deployed in the organisation. A well-defined information security policy is in place and available on the organisation's Intranet. All users are required to sign-off acceptance on an annual basis and new employees are required to attend induction training where the information security policy contents are discussed.

For the past four years the organisation deployed a comprehensive information security awareness programme. It included, among others, information security web-based training that all employees had to complete; monthly e-mails and posters covering key information security messages; presentations to business units regarding information security requirements; information security representation in the system development meetings; and regular reporting of information security issues or implementations to the Executive Risk Director. The South African firm is audited by the head office on an annual basis. The objective of this audit is to ensure that all minimum information security requirements are met by the organisation so as to allow the South African practice's connectivity to the organisation's global network.

The organisation welcomed the information security culture survey as another vehicle in driving information security awareness and an attempt to identify ways in which to further improve its protection of information assets. The ISO's objective with the information security culture assessment was to use its results as input for the information security awareness programme being

planned for the following year.

7.4 STEP 1: INFORMATION SECURITY CULTURE ASSESSMENT PLANNING AND PREPARATION

7.4.1 Step 1.1: Involve stakeholders

The information security culture assessment was launched as one of the projects within the organisation. The project was initiated through a formal project introduction meeting aimed at obtaining buy-in from relevant stakeholders and discussing the project plan. As part of this meeting, the concept of information security culture was discussed, as well as the approach that would be followed in conducting the survey. The stakeholders involved consisted of representatives from various departments – Information Technology, Information Security, Risk Management and Human Resources. The project sponsor was the Executive Risk Director. The various stakeholders assisted with the survey communication, technology set-up and coordination of the project across the target population to ensure that the required responses were obtained.

7.4.2 Step 1.2: Develop an information security culture assessment instrument

The author of this thesis used an existing information security culture assessment instrument (see Appendix B, Martins & Eloff 2002) as a starting point to design the assessment instrument for this empirical study. The existing instrument assesses information security culture and is based on a framework developed by Martins and Eloff for information security culture (Martins & Eloff 2002). It aided the researcher of this study to use statements that related to the dimensions of ISCF. Martins and Eloff used a similar approach to conduct the survey and thus it was possible to use the questionnaire in the context of this research.

The existing assessment instrument's layout, scales for answering and question structure were taken into account in preparing an enhanced information security culture assessment instrument for this research project.

Consideration was first of all given to the maturity of the information security function in the organisation. Discussions were held with the ISO and the ISF to gauge the effectiveness and efficiency of information security controls that had been deployed in the organisation. Insight was also obtained into the way in which management perceives employees' commitment to information security and the latter's compliance with the information security policy. The general perception was that employees are committed and willing to comply with the information security policy, and that the information security awareness programme was adequate in reinforcing the responsibilities of employees towards the protection of information assets.

The information obtained in the discussions was used to structure some of the statements used in the information security culture assessment instrument (e.g. employees were asked which of the current information security awareness actions they found to be the most effective in communicating messages). The assessment instrument statements also had to incorporate the information security components of the Information Security Culture Framework (ISCF), as discussed in Chapter 5. This ensured that the researcher was in actual fact measuring the information security culture status in the organisation as defined in this research study – thereby meeting content validity requirements.

7.4.3 Step 1.3: ISCF validation

Content validity of the information security culture assessment instrument used in the empirical study was ensured by preparing two or more statements for each of the components in the ISCF. In some instances it was possible to use the statements of the initial assessment instrument as they corresponded with the components of the framework. However, the initial assessment instrument was not designed based on the ISCF, as the latter was developed

and adjusted over a period of time specifically for this research project. Newly formulated statements were therefore compiled to address each component of the ISCF, thereby enhancing the initial assessment instrument.

The empirical study assessment instrument statements were discussed with industry experts in South African organisations to confirm the practicality of the statements. The five organisations that participated were from the financial service, consumer market and energy and natural resource sectors. In order to protect the confidentiality of the organisations, the company and individual names are not published. All the organisations make use of information technology (IT) for their key business processes and require information security controls to comply with regulations, protect client information and to ensure that their IT systems are always available.

The Information Security Officer, Information Technology personnel, Data Governance Officer, Risk and Compliance Officer, Information Security Consultants, a Human Resources representative, a Marketing or Communication Representative, an Internal Auditor, as well as general computer users were some of the industry expert employees who took part in the discussions. Each of these individuals interacts with information security, being involved in management, implementation, communications, auditing and/or compliance.

The discussions kicked off with an introduction to information security culture and the process proposed to assess it. The information security culture assessment instrument was also introduced and the objective thereof was explained. The statements were then discussed and tailored based on the input received. Most of the changes involved adding examples to explain statements, as well as customising the language used to correspond with each organisation's terminology. The example below illustrates the explanation of the monitoring techniques that the organisation uses (see words in italics). The words in brackets are alternatives, depending on the organisation's own jargon. In some organisations employees feel somewhat sensitive when the word 'monitoring' is used. Thus, the replacement of words

such as 'auditing' or 'review' could be considered when customising the assessment instrument for a specific organisational environment.

I feel comfortable that ABC makes use of electronic (online computer) monitoring (auditing) techniques to monitor (review) whether I comply with the information security policy *(e.g. Internet sites visited, identification of weak passwords or audit trails).*

The empirical study assessment instrument was finalised based on the components in the ISCF, the input from industry and the discussions held in the empirical study organisation. Its content is valid as it incorporates all the component categories and components of ISCF that serve as the theoretical base to assess information security culture in an organisation.

The assessment instrument is divided into the three sections listed below.

a. Knowledge questions

A section containing knowledge questions (Table 7.1, questions 1 to 13) is included to determine how much knowledge employees have about information security. This section contains organisation-specific questions regarding the information security awareness programme or issues about which management required information and that did not relate specifically to the ISCF. For the majority of the questions a "Yes/No" scale is used.

b. Information security culture statements

This section assesses the perception of employees about the seven ISCF component categories. See Table 7.1 questions 14 to 85.

A Likert scale (strongly agree, agree, unsure, disagree, strongly disagree) was used to provide a range of options among which respondents could choose to answer the statements in this section. The scale indicates the respondents'

degree of agreement or disagreement with the statements made in each case (Dillon, Madden & Firtle 1993:292). The option "unsure" was used as it was preferred by the organisation participating. "Neutral", "don't know" or "not applicable" can also be used.

c. Biographical questions

Biographical or demographical questions are added to the information security culture assessment instrument to segment the data and draw comparisons within the population, for instance with regard to job levels or length of service (see example below).

86. Length of service in ABC?
❍ 1 to 3 years
❍ 4 to 5 years
❍ 6 to 10 years
❍ More than 10 years

Please refer to Table 7.1 for the statements of the information security culture assessment instrument designed for the empirical study. The first column outlines the information security culture statements grouped in dimensions and sub-dimensions based on the ISCF components. The second column lists the theoretical reference used as input and guidance to develop the statements, The third column indicates through an inclusion tick (✓) whether the statement was developed based on input obtained mostly from industry as opposed to theory. The context of all the statements in the questionnaire is however based on the theoretical dimensions and sub-dimensions of the ISCF, and thereby helps to establish content validity.

Table 7.1 Information security culture questionnaire statements

Questionnaire statements	Theoretical reference	Industry input
Knowledge Statements		
1 ABC has a written information security policy.	ISO/IEC 17799:2005	
2 I have read the information security policy sections that are applicable to my job.		✓
3 I know where to get a copy of the information security policy.		✓
4 I understand the information security policy.		✓
5 I know what information security is.	ISO/IEC 17799:2005	
6 I know what my responsibilities are regarding information security.		✓
7 I am informed of information security requirements to protect information	ISO/IEC 17799:2005; McIlwraith 2006; SOGP 2003	
8 I know what the risk is when opening e-mails from unknown senders, especially if there is an attachment.		✓
9 I know how to use the anti-virus software to scan for viruses (e.g. when I download files from the Internet).	ISO/IEC 17799:2005	
10 When I leave my computer I always lock the screen.	ISO/IEC 17799:2005	
11 At the end of the day I ensure that there are no confidential documents left in my working area.	ISO/IEC 17799:2005	
12 Which of the following do you regard as information? Select ALL that apply • Hard copy documents (e.g. printed reports) • Electronic documents • Faxes • Business discussions • Telephone conversations • E-mail • Voicemail messages • Documents saved on a PDA (personal digital assistant) or mobile phone • Instant messaging conversations • Information published on the Internet or Intranet • All of the above		✓

Questionnaire statements	Theoretical reference	Industry input
13 How do you prefer to receive information security messages? Select ALL that apply • Induction training • The Intranet • Posters • E-mail messages • Discussion groups • Business unit presentations • Hands on training sessions • SMS messages • Web based training • Articles in the New Frontiers • Plasma screens • Promotional items • Video's		✓
Information Security Culture Statements		
Dimension: Leadership and Governance		
Sub dimension: Sponsorship		
14 Management in my business unit adheres to the information security policy.	Schiesser 2002; SOGP 2003	
15 The protection of information is perceived as important in my business unit.		✓
16 Management perceives information security as important to protect information.	Tessem & Skaraas 2005	
17 Senior management in ABC is committed to protect confidential information.	Schiesser 2002; SOGP 2003; Tessem & Skaraas 2005	
Sub-dimension: Strategy		
18 I believe it is necessary to protect information to achieve the business strategy of ABC.	CISA 2005; Sherwood, Clark & Lynas 2005	
19 I believe ABC pays adequate attention to an information security strategy in order to protect information.	CISA 2005; Sherwood, Clark & Lynas 2005	
20 The information security controls implemented by ABC support the business strategy.	CISA 2005; Sherwood, Clark & Lynas 2005	
Sub-dimension: Governance		
21 ABC is committed to information security in order to protect information.	Von Solms 2006; Tessem & Skaraas 2005	
22 Information security controls are adequately deployed in ABC to protect information.		✓
23 I understand how information security is managed in ABC to protect information.		✓
Sub-dimension: Risk Management		
24 It is important to understand the threats and vulnerabilities to information assets in my work environment.	Hall 1998	
25 Threats to information assets are controlled adequately in my business unit.	Hall 1998	
26 I believe the risk management processes of ABC are	Hall 1998	

Questionnaire statements	Theoretical reference	Industry input
adequate to identify risks that could negatively impact on the integrity, confidentiality and availability of our information.		
Sub-dimension: Return on Investment		
27 I believe the firm commits enough time to protect information.		✓
28 I believe the firm commits enough people to protect information.		✓
29 I believe the firm commits enough money to protect information.		✓
30 Investing in information security should be seen as a necessary future investment.		✓
Sub-dimension: Legal and Regulatory		
31 I believe ABC complies with regulatory requirements relating to information security (e.g. Sarbanes Oxley Act, PROATIA and ECT Act) that is applicable to our business.	Donaldson 2005	
32 Management provides me with guidance to implement the regulatory requirements (e.g. client confidentiality and retention of information) pertaining to information security that are required in my daily work.		✓
Dimension: Security Policies		
Sub-dimension: Policies, Procedures, Standards and Guidelines: Statement		
33 The information security policy is applicable to information I use in my daily duties.	Von Solms & Von Solms, 2003; Gaunt 2000	
34 The contents of the information security policy are easy to understand.	Von Solms & Von Solms, 2003; Gaunt 2000	
35 The information security policy, procedures and guidelines clearly state what is expected of me to safeguard information.	Von Solms & Von Solms, 2003; Gaunt 2000	
Sub-dimension: Code of / Best Practice (including Certification)		
36 I believe the information security controls deployed in ABC compare favourably with best practice guidelines to secure information assets.		✓
37 I believe it is necessary that information security controls implemented in ABC are in line with best practice guidelines to secure information assets.		✓
Dimension: Security Management and Organisation		
Sub-dimension: Program Organisation		
38 I believe it is necessary to commit time to protect information.		✓
39 I believe it is necessary to commit people to protect information.		✓
40 I believe it is necessary to commit money to protect information.		✓
41 I believe the Information Security Group (ISG) in ABC has adequate authority to ensure the implementation of information security controls.	McCarthy & Campbell 2001	
42 There are adequate information security specialists/coordinators throughout ABC to ensure		✓

Questionnaire statements	Theoretical reference	Industry input
the implementation of information security controls.		
43 I believe the Information Security Group (ISG) adequately assists in the implementation of controls to protect information of ABC.	McCarthy & Campbell 2001	
Dimension: Security Program Management		
Sub-dimension: Monitor and Audit		
44 Information security should be part of key performance measures for employees of ABC.	Vroom & Von Solms 2004	
45 Employees should be monitored on their compliance to information security policies and procedures (e.g. measuring the use of e-mail, monitoring which sites an individual visits or what software is installed on computers).		✓
46 I feel comfortable that ABC makes use of electronic monitoring techniques to monitor if I comply with the information security policy (e.g. Internet sites visited, identification of weak passwords or audit trails).		✓
Sub-dimension: Compliance		
47 My business unit enforces adherence to the information security policy.	Von Solms 2005; Vroom & Von Solms 2004	
48 Employees in our business unit adhere to the information security policy.	Von Solms 2005; Vroom & Von Solms 2004	
49 Action should be taken against anyone who does not adhere to the information security policy (e.g. if they share passwords, give out confidential information Of visit prohibited Internet sites).		✓
50 I should be held accountable for my actions if I do not adhere to the information security policy.	Von Solms 2005; Vroom & Von Solms 2004	
Dimension: User Security Management		
Sub-dimension: Education and Training		
51 The contents of the information security policy were effectively explained to me.	Dojkovski, Lichtenstein, Warren 2006	
52 I believe there is a need for additional training to use information security controls in order to protect information.		✓
53 I believe the information security awareness initiatives are effective.	Dojkovski, Lichtenstein, Warren 2006; ISO/IEC 17799:2005	
54 I received adequate training to use the applications I require for my daily duties.	Dojkovski, Lichtenstein, Warren 2006; ISO/IEC 17799:2005	
Sub-dimension: Trust		
55 I believe that management communicates relevant information security requirements (e.g. what Internet usage is allowed, how to make back ups, security usage of removable media such as USB's / PDA's) to me.		✓

Questionnaire statements	Theoretical reference	Industry input
56 I believe the Information Technology business unit *implements information security controls (e.g.* restricting access to secure areas, controlling access to computer systems, preventing viruses).		✓
Sub-dimension: Employee Awareness		
57 Information security is necessary in my business unit to protect information.	McIlwraith 2006	
58 The employees in our business unit perceive information security (e.g. sharing confidential information) as important to protect information.	McIlwraith 2006	
59 I am aware of the information security aspects relating to my job (e.g. when to change my password or which information I work with is confidential).	McIlwraith 2006	
Sub-dimension: Ethical Conduct		
60 I accept responsibility towards the protection of information.	Cardinali 1995	
61 I think it is important to regard the work I do as part of the intellectual property of ABC.		✓
62 I believe it is important to take care when talking about confidential information in public places.		✓
63 I believe that e-mail and Internet access are for business purposes and not personal use.		✓
64 I believe everyone in ABC complies with copy right laws.		✓
65 I believe that sharing of passwords should be used to make access to information easier.		✓
Sub-dimension: Privacy		
66 I believe that third parties who have access to confidential information preserve the confidentiality thereof.	ISACA 2005; SOGP 2003	
67 There are clear directives on how to protect sensitive (confidential) client information.	ISACA 2005; SOGP 2003	
68 There are clear directives on how to protect sensitive (confidential) employee information.	ISACA 2005; SOGP 2003	
69 I believe that management keeps my private information (e.g. salary or performance appraisal information) confidential.	ISACA 2005; SOGP 2003	
Dimension: Technology Protection		
Sub-dimension: Asset Management		
70 My business unit is protecting its information assets adequately (i.e. locking away of confidential documents or files).	ISO/IEC 17799:2005	
71 I believe that the information I work with is protected adequately.	ISO/IEC 17799:2005	
Sub-dimension: System Development		
72 I believe the process followed by ABC to ensure information security is considered when new systems are developed, is adequate.	ISO/IEC 17799:2005	

Questionnaire statements	Theoretical reference	Industry input
73 I believe that the information security controls (e.g. passwords) of the applications I use in my daily duties are adequate.	ISO/IEC 17799:2005	
Sub-dimension: Technical Operations		
74 The Information Technology Services (ITS) business unit employees believe information security is important.		✓
75 The protection of information is predominantly the responsibility of the Information Technology Services (ITS) business unit.		✓
Sub-dimension: Incident Management		
76 I believe the incident management process of ABC is effective in resolving information security incidents.	ISO/IEC 17799:2005	
Sub-dimension: Physical and Environmental		
77 The information assets I work with need to be secured.	ISO/IEC 17799:2005	
78 I feel safe in the business unit I work in.		✓
79 I believe the building I work in is safeguarded adequately to protect information assets.	ISO/IEC 17799:2005	
Sub-dimension: Business Continuity Management		
80 I believe my business unit will be able to continue its daily operations if there is a disaster (e.g. fire, explosion or flood) resulting in the loss of systems, people and/or premises.	ISACA 2003; ISO/IEC 17799:2005	
81 I know what to do in the event of a disaster resulting in the loss of computer systems, people and/or premises.	ISACA 2003; ISO/IEC 17799:2005	
Dimension: Change		
Sub-dimension: Change		
82 I accept that some inconvenience (e.g. locking away confidential documents, making back ups or changing my password regularly) is necessary to secure important information.		✓
83 I am prepared to change my working practice in order to ensure the protection of the information assets (e.g. systems and information in paper or electronic format).		✓
84 Changes in our business unit to secure information are accepted positively (e.g. using passwords for hand held devices such as PDA's or using additional passwords to log on to my computer and applications).	Tessem & Skaraas 2005	
85 I am informed in a timely manner as to how information security changes (e.g. policy changes, patches to computer software or additional passwords) will affect me.		✓

The assessment instrument was accompanied by a cover letter that explained why employees had to complete the survey, what would be done with the feedback, how long it would take to complete a report, and that the responses would be anonymous.

A discussion meeting was conducted with the ISO to ensure that the assessment instrument terminology, layout and design were in line with the requirements of the organisation. The biographical questions were finalised based on the selected target population. Apart from the South African office, offices in Swaziland and Botswana were also included. The biographical questions included length of service; job level; business unit; and geographical area. The information security culture assessment instrument was finalised and signed off by the ISO to be used in the assessment.

7.4.4 Step 1.4: Determine population and sample size

All the company's employees in South Africa, Swaziland and Botswana – altogether 3 055 employees – were included in the population and had to complete the assessment instrument. This method is referred to as convenience sampling (Brewton & Millward 2001:118). The job levels ranged from administrative employees to executives.

7.4.5 Step 1.5: Conduct a pilot survey

To ensure that the empirical study was conducted in a professional manner and that the process used to deploy the survey was effective, an initial survey was conducted in a South African financial organisation that was willing to participate in the research project. The information security culture questionnaire was sent out to all employees in selected business areas, involving altogether 12 572 employees. This method is referred to as convenience sampling (Brewton & Millward 2001). Overall, a representative number of 4 735 employees participated in the survey, which was a more than adequate sample.

The survey results were analysed using Survey Tracker (2005). SAS (2008) was used for the validation of the assessment instrument. The respondents represented all job levels in the organisation: executive and senior managers (3.97%), department managers and supervisors (21.94%), operational job staff (64.16%) and technology staff (8.51%). Most respondents had worked for the organisation for more than ten years (32.06%) or for between 5 and ten years (23.59%), 77.4% worked at head office, and the rest at branch offices. Responses were received from all nine provinces in South Africa, with the majority from Gauteng (62.09%), followed by the Western Cape (12.61%) and KwaZulu-Natal (9.17%).

This initial survey can be regarded as a pilot study for the research project. The objective of this pilot survey was to

- determine the value of an information security culture assessment in the industry;
- identify statements that users did not understand and that had to be reworded or removed;
- ensure that statements are practical;
- experiment with the process of conducting an information security culture assessment; and
- try out the statistical analysis to be used to validate the assessment instrument.

The assessment instrument, previously referred to as the "existing information security culture assessment instrument" (see Appendix B) was used in the pilot study. Please refer to Appendix D for a paper published discussing the pilot study organisation and how the assessment was conducted.

The assessment instrument statements were improved and the data was used to conduct a reliability and validity analysis. The results of the reliability and validity analysis were used to revise the existing information security culture assessment instrument and to provide a valid and reliable assessment instrument based on the statistical analysis. The limitations of the pilot study and the existing information security culture assessment instrument were that

the assessment instrument did not address all the components defined in the ISCF. This problem was rectified by adjusting the assessment instrument after the first survey had been conducted. A second survey was therefore necessitated. The lessons learned from the initial survey were heeded and the same assessment process and statistical analysis were applied in order to validate the information security culture assessment instrument designed for the empirical study.

7.4.6 Step 1.6: Select appropriate assessment technology

Survey Tracker (2008) was used as the survey software to distribute, capture and conduct the survey analysis. The information security culture assessment instrument was designed in html format in Survey Tracker according to the scientific rules of scales and question types built into the software. The assessment instrument files were saved on one of the secure servers of the organisation to enable employees to complete the assessment instrument while being logged on to the organisation's network.

7.5 STEP 2: INFORMATION SECURITY CULTURE ASSESSMENT ADMINISTRATION

7.5.1 Step 2.1: Communicate information security culture assessment

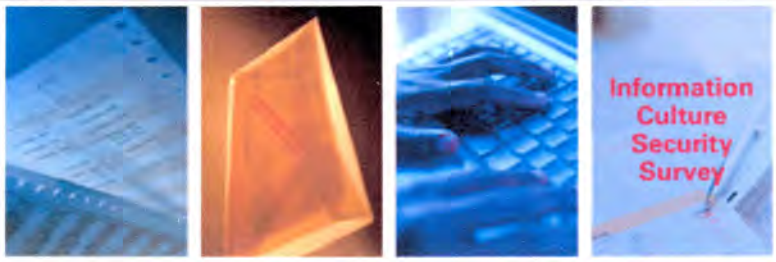
A communication e-mail was sent out to all employees from the Executive Risk Partner explaining the objective of the survey (see Figure 7.1 for the e-mail.) The survey ran for a period of two weeks. Further reminder e-mails were sent to employees from the Information Security mailbox and posters were put up in all offices across the country to remind employees to complete the survey.

Figure 7.1 Information security culture assessment communication

Information Security Culture Survey

Internal Use Only

November 2007



The information security culture survey

The confidentiality, integrity and availability of our employee and client information are extremely important. ABC is always looking at new and innovative ways to improve the protection of our information assets through information security.

This survey hopes to determine ABC employees' attitude and perception towards information security.

To help us maintain and improve our current processes, we need your feedback through the information security culture survey. No personal information will be requested from you and your response will be anonymous.

Complete the survey

The survey will take approximately 20 minutes to complete. Please read the instructions carefully, do the survey and click on the submit button at the end of the questionnaire. You have to do the entire survey in one session. To do the survey you have to be in the office, dialled up (using a RAS token) or connected by Virtual Private Network (VPN). Unfortunately, you cannot use a datacard. *The survey must be completed by Friday, 16 November 2007.*

Please click here to access the survey http://xxx/InfoSecSurvey/InfoSecSurvey.htm

The results will be analysed and used by the Information Security Group (ISG) to improve the protection of our information assets.

Thank you for taking the time to complete the survey.

Regards,

xxx

Executive Partner Risk Management

Any questions relating to information security can be sent to ZA-FM SA INFORMATION SECURITY. To learn more about information security policies, issues and ISG services visit us at http://www.xxx

7.5.2 Step 2.2: Send out information security culture assessment instrument

In collaboration with the IT department, a link to the assessment instrument was created that could be e-mailed to employees to complete the survey electronically (Figure 7.1).

7.5.3 Step 2.3: Monitor responses

For the purpose of the empirical study, the completed assessment instrument responses were automatically saved in a file on the organisation's server. During the survey period the responses were tracked to ensure that a statistically representative response was obtained for each biographical area in which the data would be segmented. Table 7.2 provides a summary of the organisation's business units, the number of employees in each, the statistically representative sample required and the actual response obtained. The method designed by Krejcie and Daryle (1970) (see Table 7.2) was used to determine the required sample size. In four business units the response rate was not representative. Trends were considered for these divisions when the results were analysed. It was recommended to the organisation to conduct further focus groups in these divisions to confirm the results.

Table 7.2 Information security culture survey – representative sample

Business Units	Total number of employees	Sample required based on method of Krejcie & Daryle	Actual responses	Representative (Yes / No)
Business Unit A	1455	304	384	Yes
Business Unit B	261	156	118	No
Business Unit C	355	182	152	No
Business Unit D	75	63	49	No
Business Unit E	579	230	252	Yes
Business Unit F	5	5	18	Yes

Business Units	Total number of employees	Sample required based on method of Krejcie & Daryle	Actual responses	Representative (Yes / No)
Business Unit E	205	134	70	No
No response	N/a	N/a	1	N/a
Other	N/a	N/a	41	N/a
Overall	2935	239	1085	Yes

When a validity test is conducted, the commonly accepted criterion is to have at least 100 respondents or five times the number of responses compared to the number of questions in the assessment instrument (Martins 2000). The preferred criterion is to have at least ten times the number of responses so as to ensure that the conclusions drawn from the sample data are not sample specific and would allow generalisation of the findings (Martins 2000). The information security culture assessment instrument consists of 72 information security culture questions that are used in the statistical analysis. Overall, a representative number of 1 085 employees participated in the survey, thus a more than adequate sample.

7.6 STEP 3: INFORMATION SECURITY CULTURE ASSESSMENT DATA ANALYSIS

7.6.1 Step 3.1: Conduct a statistical analysis

Survey Tracker was used to compile different reports in order to interpret the empirical study results. The mean, percentage favourable, neutral and unfavourable responses for each statement were analysed. To obtain the percentage for favourable responses, the strongly agree and agree responses were grouped together. The strongly disagree, disagree responses and unsure responses were also grouped together to constitute the percentage of unfavourable responses. This was done to present the results in a more easily understandable format for the organisation.

The respondents represented all job levels in the organisation, from top management (director) (8.2%), senior management (12.8%), management (16.9%), supervisor (17.9%), trainee (24.2%) up to clerical or support staff (19.9%) (see Figure 7.2). The largest number of respondents had worked for the organisation for between one and three years (56.7%), or between six and ten years (16.9%) (see Figure 7.3). Responses were received from all the geographical areas. with most coming from Johannesburg (52.4%) and Pretoria (12.1%), followed by Cape Town (10.5%) (see Figure 7.4).

Figure 7.2 Job levels

87. What is your job level?

Response	Frequency	Percentage
Top Management (Director)	89	8.2%
Senior Management (Senior Manager)	139	12.8%
Management	183	16.9%
Supervisory	194	17.9%
Trainee	263	24.2%
Clerical or Support Staff	216	19.9%
No Response	1	0.1%

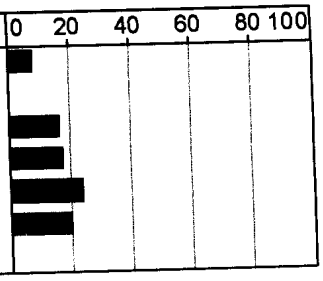


Figure 7.3 Length of service

86. Length of service in ABC?

Response	Frequency	Percentage
1 to 3 years	615	56.7%
4 to 5 years	123	11.3%
6 to 10 years	183	16.9%
More than 10 years	160	14.7%
No Response	4	0.4%

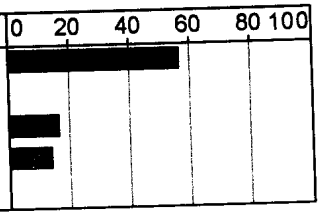
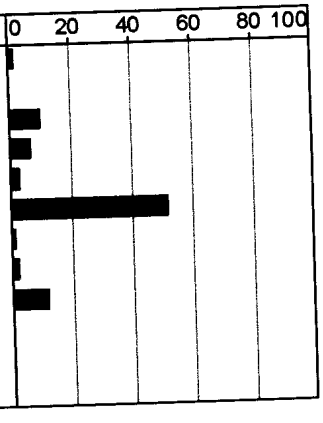


Figure 7.4 Geographical areas

89. In which geographical area is your office located?

Response	Frequency	Percentage
Bloemfontein	26	2.4%
Botswana	33	3.0%
Cape Town	114	10.5%
Durban	81	7.5%
Eastern Cape	38	3.5%
Johannesburg	569	52.4%
Nelspruit	19	1.8%
Polokwane	32	2.9%
Pretoria	131	12.1%
Secunda	8	0.7%
Swaziland	31	2.9%
No Response	3	0.3%



The knowledge questions were analysed separately from the culture questions, as these two sets of questions each had different objectives. The knowledge questions are used to provide background in analysing the culture questions and they focus on what employees "know". The information security culture questions are used to measure the level of information security culture in the organisation and focus on the opinion and perception of employees regarding the information security components defined in the ISCF.

7.6.2 Step 3.2: Construct validity

The seven dimensions (component categories) of the information security culture assessment instrument – and not the sub-dimensions (components) – are used for the confirmatory factor analysis, as some of the sub-dimensions have less than three statements and are too small to perform the analysis on.

Table 7.3 lists the three attributes that are assessed for the factor analysis in column one, while the corresponding value derived from the statistical analysis is listed in column two. Column three provides a summary of the acceptance criteria as described by Schermelleh-Engel, Moosbrugger and Müller (Shermelleh-Engel et al. 2003) and Brewerton and Millward (Brewerton & Millward 2001: 168). The fourth column indicates whether the factors are accepted, based on the criteria.

It is clear from the results that the GFI and AGFI are higher than the minimum accepted value. The RMR is also very close to 0. The results indicate that the theoretical model (i.e.the ISCF) can be accepted and that there is a *good fit* between the theoretical model (ISCF) and the empirical data. This implies that the criteria for construct validity are met, using the SEM analysis technique.

Table 7.3 Results of the SEM analysis

Attribute	Value of analyses	Criteria		Accepted
		Good fit	Acceptable fit	
Goodness of Fit Index (GFI)	0.9982	.95 ≤ GFI ≤ 1.00	.90 ≤ GFI ≤ .95	Yes, good fit
Adjusted for Goodness of Fit Index (AGFI)	0.9981	.90 ≤ AGFI ≤ 1.00	.85 ≤ AGFI ≤ .90	Yes, good fit
Root Mean Square Residual (RMR)	0.0798	Close to zero		Yes

7.6.3 Step 3.3: Reliability

Next, the reliability of each factor was determined by means of an item analysis (Cronbach's alpha). This was conducted on a dimension level in order to establish the Cronbach alpha of each dimension based on the theoretical framework (model), namely ISCF. Table 7.4 lists the seven factors with the corresponding Cronbach's alpha value, the number of statements per factor and the statement number as in the assessment instrument. All the values meet the minimum accepted criteria and are above 0.7. This analysis confirms the internal consistency and reliability of the assessment instrument.

Table 7.4 Results of the reliability analysis

Factors	Cronbach's alpha	Number of items/ statements/ comments	Statements
Factor 1: Leadership and Governance	0.946	17	14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30
Factor 2: Security Management and Operations	0.858	8	31, 32, 38, 39, 40, 41, 42, 43, 44
Factor 3: Security Policies	0.859	5	33, 34, 35, 36, 37
Factor 4: Security	0.814	7	44, 45, 46, 47, 48, 49, 50

Factors	Cronbach's alpha	Number of items/ statements/ comments	Statements
Program Management			
Factor 5: User Security Management	0.837	19	51, 52, 53, 54, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81
Factor 6: Technology Protection and Operations	0.841	12	55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66
Factor 7: Change	0.740	4	82, 83, 84, 85

7.7 INFORMATION SECURITY CULTURE ASSESSMENT REPORT-WRITING AND FEEDBACK

7.7.1 Step 4.1: Compile an information security culture assessment feedback report

A report was compiled for the organisation, highlighting the key developmental areas and proposed action plans. The report was presented to management who used the developmental areas as the focus for their planned awareness programme. (Refer to Appendix C for the statistical report on the overall data which was used as input for the feedback report.) The next few paragraphs provide an overview of the results of the knowledge and information security culture statements, as well as the key recommendations.

The overall results of the 13 information security culture knowledge questions are displayed in Figure 7.5. The first column lists the questions and the second column the number of employees who responded to the question. The third column is a graphical representation of the responses indicating in green the percentage of employees who agreed with the question and in red the percentage of employees who selected "No". The last two columns provide the percentage figures of the respondents who selected "Yes" and "No" respectively.

The questions are ranked from the highest positive statement to the lowest. From the results it is evident that almost all employees (99.8%) are aware of the organisation's information security policy, but 17% does not know where to obtain a copy. A total of 46.3% of employees do not know how to use the anti-virus software to scan for viruses. The reason for this could be that the organisation configured the anti-virus software to automatically scan for viruses. The overall awareness average is 89.9%, indicating that most employees are aware of the information security knowledge concepts, just as the organisation expects from them.

Figure 7.5 Statements about information security culture knowledge

Questions	Count	Category Percentages 0 20 40 60 80 100	Yes	No
1. ABC has a written information security policy.	1084	99.8%	99.8%	0.2%
5. I know what information security is.	1081	99.1%	99.1%	0.9%
8. I know what the risk is when opening e-mails from unknown senders, especially if there is an attachment.	1084	98.5%	98.5%	1.5%
6. I know what my responsibilities are regarding information security.	1083	97.1%	97.0%	3.0%
7. I am informed of information security requirements to protect information.	1082	95.6%	95.6%	4.4%
10. When I leave my computer I always lock the screen.	1083	93.2%	93.2%	6.8%
4. I understand the information security policy.	1082	91.7%	91.7%	8.3%
11. At the end of the day I ensure that there are no confidential documents left in my working area.	1083	90.3%	90.3%	9.7%
2. I have read the information security policy sections that are applicable to my job.	1084	87.0%	87.0%	13.0%
3. I know where to get a copy of the information security policy.	1084	83.0%	83.0%	17.0%
9. I know how to use the anti-virus software to scan for viruses (e.g. when I download files from the Internet).	1081	46.4% 53.7%	53.7%	46.3%
Overall Averages	1082.8	89.9%	89.9%	10.1%

Figure 7.6 portrays the overall results of the seven information security culture dimensions. The two dimensions were the employee perceptions where the most unfavourable were Technical Protection and Operations, and User

Security Management. Leadership and Governance and Security Policies were the most favourable or positive dimensions.

Figure 7.6 Results for the information security culture dimensions

Groups	Count	Mean	Category Percentages 0 20 40 60 80 100	Favorable	Neutral	Unfavorable
Leadership and Governance	1081.1	4.20	89.7%	89.7%	7.4%	2.9%
Security Policies	1076.0	4.13	89.5%	89.5%	8.5%	1.9%
Security Management and Organisation	1080.6	4.08	84.0%	84.0%	13.3%	2.7%
Change	1076.8	4.07	89.0%	89.0%	6.8%	4.1%
Security Program Management	1079.4	3.95	83.1%	83.1%	10.5%	6.4%
User Security Management	1078.3	3.82	76.0%	76.0%	11.8%	12.2%
Technology Protection and Operations	1080.0	3.75	72.8%	72.8%	15.3%	11.9%
Overall Averages	1079.4	3.98	82.0%	82.0%	10.9%	7.2%

Notes:

Count = Number of respondents. This is an accumulated figure. All respondents did not respond to all statements in each dimension.
Mean = The total of the scores divided by the number of responses.

Categories / Scales

Green (Favourable %) = 5 - Strongly agree, 4 - Agree
Yellow (Neutral %) = 3 - Uncertain
Red (Unfavourable %) = 2 Disagree, 1 - Strongly disagree

Each of the information security culture statements were further investigated to identify the 10 highest (most favourable) and 10 lowest (least favourable) statements. The ten highest statements could be leveraged on to aid with action plans. The ten lowest statements are identified as a starting point to address the most critical areas first. These statements are addressed to improve employee perceptions and, as such, the information security culture in the long term.

The ten highest-ranked statements for the overall results, based on the percentage figures, are:

1. I believe it is important to take care when talking about confidential information in public places. (99.3%)
2. I believe it is necessary to protect information to achieve the business strategy of ABC. (99.2%)
3. I believe it is necessary to commit time to protect information. (99.0%)

4. I believe it is necessary to commit people to protect information. (98.9%)
5. I accept that some inconvenience (e.g. locking away confidential documents, making backups or changing my password regularly) is necessary to secure important information. (98.6%)
6. I accept responsibility for the protection of information. (98.5%)
7. It is important to understand the threats to and vulnerabilities of information assets in my work environment. (98.3%)
8. I am aware of information security aspects relating to my job (e.g. when to change my password or whether the information I work with is confidential. (97.9%)
9. Investing in information security should be seen as a necessary future investment. (97.4%)
10. I believe it is necessary to commit money to protect information. (97.4%)

The ten lowest ranked statements for the overall results based on the percentage figures are:

1. I believe there is a need for additional training to use information security controls in order to protect information. (14.2%)
2. I believe that third parties who have access to confidential information preserve the confidentiality thereof. (40.8%)
3. I know what to do in the event of a disaster resulting in the loss of computer systems, people and/or premises. (44.2%)
4. I believe everyone in ABC complies with copyright laws. (48.4%)
5. The protection of information is predominantly the responsibility of the Information Technology Services (ITS) business unit. (50.0%)
6. I believe my business unit will be able to continue its daily operations if there is a disaster (e.g. fire, explosion or flooding) resulting in the loss of systems, people and/or premises. (50.0%)
7. I believe the incident management process of ABC is effective in resolving information security incidents. (56.1%)

8. There are adequate information security specialists/coordinators throughout ABC to ensure the implementation of information security controls. (64.4%)
9. I believe that management communicates to me relevant information security requirements (e.g. what Internet usage is allowed, how to make backups, security usage of removable media such as USBs/ PDAs). (64.9%)
10. The contents of the information security policy were effectively explained to me. (71.1%)

Table 7.5 provides a summary of three of the key recommendations for illustration purposes. The recommendations are based on the lowest statements in the overall information security culture report. These statements were further analysed in terms of differences and significant differences between business areas, job levels and geographical areas for each statement.

Empirical study

Table 7.5: Recommendations for information security culture

Statement	Recommendation
I believe there is a need for additional training in the use of information security controls in order to protect information. (14.2%)	Only 14.2% of the organisation's employees felt comfortable that they received adequate training in information security. 71.5% of the employees therefore indicated that there is a need for additional training. However, 77.4% of employees felt that they received adequate training to use applications they require for their daily duties. From the knowledge questions it was evident that most employees understand what is meant with information security and 71.1% of employees indicated that the Information Security policy was effectively explained to them. **Actions**: • Top management believed more strongly that there is a need for additional training compared to trainees. This could be as a result of top management's understanding of the business risk the organisation faces in terms of information security. This situation could be further investigated by means of focus group discussions with top management in Botswana, Nelspruit, Johannesburg and Pretoria who were significantly more negative compared to for instance Bloemfontein who was the most positive in this regard. • Respondents from the Human Resource department were significantly more negative compared to the other departments. A focused training session could be considered for them. • The information security training that is developed should focus on the practical usage of information security controls. The training format used for applications should be investigated to determine if the same format would be effective for information security. Web-based training could be considered as users had a preference for this format.
I believe that third parties who have access to confidential information preserve the confidentiality thereof. (40.8%)	Only five per cent of employees indicated that guidelines to protect sensitive information were not adequate. Employees perhaps doubted that third parties would protect information as they might not be aware of the process followed for third parties or are aware of instances where third parties have not preserved the confidentiality of confidential information. The fact that many of the respondents selected the "unsure" option may rather be the result of a lack of communication than ith third parties and the requirements third parties

Statement	Recommendation
	have to comply with. **Actions:** • Management should conduct a workshop with employees to understand the reasons why employees were negative. Workshops should specifically be conducted with the top (23.6%) and senior management (26.8%) level as these employees were significantly more negative in this regard compared to the other job levels. Workshops in the Secunda, Nelspruit and Cape Town offices should be conducted first as respondents were more negative in these offices. • Management should communicate to users the process followed for contracting with third parties and the requirements to manage information securely as well as to address the issues brought forward in the workshop. • Management should also investigate the third party process in the respective areas to ensure that it is adequate in protecting confidential information.
I know what to do in the event of a disaster resulting in the loss of computer systems, people and/or premises. (44.2%) I believe my business unit will be able to continue its daily operations if there is a disaster (e.g. fire, explosions or flooding) resulting in the loss of systems, people and/or	There is a signed-off Business Continuity plan in place, but it has not been communicated to employees yet. There is a significant difference between senior management (36.2%) and the other job levels in terms of knowing what to do in the event of a disaster. There is also a significant difference between the geographical areas in terms of the before-mentioned. Secunda (37.5%), Johannesburg (40.2%) and Durban (42%) were the most negative. Interestingly, only 36% of the respondents from IT departments believed that their business unit would be able to continue its daily operations in the event of a disaster. **Actions:** • The awareness plan should incorporate business continuity as one of the key focus areas to communicate to employees. E-mail, web-based training and the Intranet can be considered for communication as respondents indicated tl ımmunication methods. Communication initiatives should start off with senic ıt and specifically in the offices located in Secunda,

Empirical study

Statement	Recommendation
premises. (50.0%)	Johannesburg and Durban. • A simulation exercise could be considered for management with disaster scenarios to work through.

7.8 EMPIRICAL STUDY EVALUATION

The empirical study was useful in illustrating the ISCULA process. It showed that the process was practical – the organisation did not have to customise it, but could implement the steps as proposed in ISCULA. The effectiveness of ISCULA was illustrated by the logical flow of the process steps, which helped to conduct the assessment in a structured and organised manner within a defined timeframe. This further enabled the project team to compile an accurate project plan and to ensure the achievement of the various milestones set by the project team. The process helped to raise awareness about the importance of working towards a valid and reliable assessment instrument to derive data that management can use for business decisions.

A requirement of the ISCULA process is that knowledge regarding statistical analysis is required for reporting on, and interpretation of the survey data, as well as for validation of the assessment instrument. To address this, the process could be expanded to include more guidance on how to conduct statistical analyses. Alternatively, a person familiar with statistical analysis, for example an industrial psychologist or statistical analyst, should participate in the assessment as part of the project team.

The ISCULA process involves obtaining data by using a quantitative method. Since this method usually involves large numbers of respondents, the information obtained can be projected to the whole population (Dillon, Madden & Firtle 1993: 135). The information security culture level determined in the assessment can therefore also be projected to the whole organisation. The ISCULA process does not support the use of qualitative methods, as these are usually applied to smaller numbers of respondents – with the result that the information obtained cannot easily be projected to the whole population (Dillon, Madden & Firtle 1993: 135). An interview or focus group is an example of a qualitative method of research. Although ISCULA proposes the use of focus groups to confirm results where a statistical representative sample was not obtained, qualitative methods are never used to gather initial assessment

information. Qualitative methods could nevertheless be useful to obtain an understanding of users' perception of, for instance, the information security policy as illustrated through the research work of Schlienger and Teufel (2005). Thus, consideration might be given to adding a step to the ISCULA process – to review for instance audit reports and the completeness of the information security policy, and to hold discussions with the Information Security Officer aimed at obtaining additional information to interpret the assessment findings.

The developmental areas were integrated in the 2008 information security awareness programme to raise the information security culture in the organisation to a more acceptable level. It was, however, found that the project team tasked to address the developmental areas required additional input about how to address the findings and integrate them with the information security awareness programme. ISCULA could therefore be expanded to include the process that an organisation can follow to incorporate the information security culture assessment findings in its awareness plan.

The assessment instrument statements comprehensively addressed the ISCF component categories and components and ensured the content validity of the assessment instrument. Assessing a broad range of components provided a holistic view of the information security culture. The results derived from the assessment were in line with what management expected with regard to the specific components to be improved. The assessment results aided management to understand whether the components to address were on an organisational, group or individual level. The findings also guided management to focus actions in a specific department, job level or geographical area, thereby saving costs, time and resources. The ISCF was clearly effective in obtaining an understanding of the level of information security culture in an organisation. The framework further helped management to understand the context of information security culture and what specific components to address in order to improve the information security culture to a more acceptable level.

In the empirical study it was found that the organisation would have preferred more statements about information security incidents and the process followed by the organisation to resolve such incidents. This illustrates that although the information security culture assessment instrument is of a generic nature, organisations might still want to revise the assessment instrument statements, and add or remove some statements. It would mean that the ISCF might also have to be revised and that the assessment instrument would subsequently need to be validated again. ISCULA is structured in such a manner that it allows organisations to revise and adapt the assessment instrument and to eventually validate it for future use.

The statistical analysis proved that the information security culture assessment instrument was valid and reliable in assessing information security culture. This was further confirmed by the agreement of management to the developmental and positive areas identified in the assessment results. Other organisations can therefore use the same assessment instrument with confidence to assess their unique information security culture. The assessment instrument statements were found to be easily understandable for employees and the assessment instrument as a whole did not take too long to fill in.

A number of alternative statistical analyses can nevertheless be conducted to improve the information security culture assessment instrument. An exploratory factor analysis may be considered to determine whether statements can be grouped in other dimensions, which could enhance the interpretation of results and the structure of the assessment instrument. More complex SEM techniques can also be employed to create a statistical model for information security components. This could contribute to the identification of relationships between components, to perhaps revise the ISCF, and to the interpretation of the results.

It could be useful to develop a model that predicts how the information security culture or more specifically the employee behaviour could be improved. Similar models have been developed by Workman et al. (2008) and

Siponen et al. (2007). Hypotheses derived from theory such as, "If employees have read the information security policy, they would be more likely to adhere to the information security policy" can then be explored. This would be useful to practitioners to understand how each statement aids to positively influence the information security culture.

7.9 CONCLUSION

Chapter 7 presented an empirical study of an information security culture assessment conducted in a South African organisation. The objective of the assessment was to validate the process of assessing an information security culture, ISCULA, and to provide a valid assessment instrument for information security culture. Ultimately, the empirical study provided the grounds to derive data in order to validate the information security culture assessment instrument. Since an adequate number of respondents participated in the assessment, the criteria for conducting the proposed statistical analysis were met. The statistical analysis aided to design a valid and reliable assessment instrument to be used in future to assess information security culture within the context of the ISCF.

The empirical study also illustrated that an information security culture assessment is necessary in organisations to identify developmental areas and to effectively direct the organisation's actions to implement and maintain information security components. This helps the organisation to minimise the costs, resources and time spent on cultivating an acceptable level of information security culture and not to over-invest in, for instance, departments where the culture is already on an acceptable level.

Finally, ISCULA and the information security culture assessment instrument contribute towards minimising the threat that user behaviour poses to information security. They enable the organisation to direct user behaviour towards the protection of information assets, based on the outcome of the information security culture assessment. The deployment of the ISCULA

process raised awareness in the organisation regarding the protection of information assets and so contributed in cultivating an information security culture.

PART IV

CHAPTER 8

CONCLUSION

8.1 INTRODUCTION

This thesis addresses the cultivation and assessment of information security culture. The first objective is to understand how to cultivate information security culture and for this purpose an Information Security Culture Framework (ISCF) is developed. The ISCF consists of information security components that influence information security behaviour on various levels in the organisation, thereby cultivating a certain level of information security culture. Besides applying the ISCF to cultivate information security in an organisation, it also serves as the foundation for designing an information security culture assessment instrument. This instrument is incorporated in this study as part of an Information Security Culture Assessment process (ISCULA) defined by the researcher. The application of ISCULA is tested by means of an empirical study conducted in an organisation.

In this chapter the researcher revisits the research questions to evaluate the extent to which they have been addressed. This is followed by an assessment of the main contribution of the research. The chapter concludes with suggestions for future research forthcoming from this work.

8.2 REVISITING THE PROBLEM STATEMENT

The overall objective of this research study is to determine how to assess and cultivate an information security culture. The thesis therefore aims to answer the following research questions:

Research question 1: What current research perspectives are available to cultivate an information security culture?

Chapter 2 defines information security culture in order for the reader to understand the context of the research. Chapter 3 addresses the above research question by evaluating the research perspectives that are currently available and that address the cultivation of information security culture. The current research perspectives focus mostly on information security culture principles to allow the reader to understand what information security culture entails and how to ultimately cultivate such a culture. Only four of the fourteen research perspectives address an information security culture framework that can be used to cultivate information security culture. The current research attempts to provide an understanding of the different components one has to consider for information security culture. There is, however, no single research perspective that integrates information security components, organisational culture and organisational behaviour to formulate an information security culture framework that illustrates the influence of different components within the framework. This problem highlighted the need for a comprehensive information security culture framework. Such a framework can help management to understand what information security culture entails and enable them to implement the required information security components to cultivate the desired information security culture.

Research question 2: What current research perspectives and/or methods are available to make an assessment of information security culture?

Chapter 3 also investigates the available research perspectives that propose how to assess information security culture. Only three perspectives were found to address the assessment of information security culture. However, these perspectives do not specifically propose an information security culture framework on which to base the design of an assessment instrument. The researchers involved refer either to organisational behaviour frameworks, organisational culture frameworks or information security standards as the

foundation for designing an assessment instrument for information security culture. When assessing information security culture it is necessary to use an assessment instrument that is based on a theoretical framework of information security culture. This enhances the content validity of the assessment instrument and ensures that the researcher does in fact assess information security culture. The study therefore highlights the need to provide a valid and reliable assessment instrument that can be used to assess information security culture and that has been designed within the context of an information security culture framework.

Research question 3: What should an information security culture framework comprise of in order to cultivate information security culture?

This research question is partly addressed in Chapter 4 where a Comprehensive Information Security Framework (CISF) is defined. It comprises of the components that can be used by management to define information security in organisations and ultimately serves as the foundation to develop a framework for information security culture. The CISF is comprehensive and involves people, process and technology components.

The Information Security Culture Framework (ISCF) is developed in Chapter 5. It illustrates what information security culture comprises, the integration between the identified components, as well as the influence between components within the framework. The ISCF illustrates that a specific information security component has an effect on either the organisational, group or individual information security behavioural tiers. This aids organisations to understand on what level in the organisation an information security component has an impact. It points out that information security components should be implemented not only on one information security behavioural tier in an organisation, but on all three to ensure the desired outcome in terms of an acceptable level of information security culture.

Information security components influence each information security behavioural tier to ultimately cultivate the information security culture that is evident in artifacts and creations, values and assumptions. The cultivated information security culture can either contribute to protect information assets or pose a risk if it is not on an acceptable level. The ISCF can be applied in an organisation to practically encourage employee behaviour to protect information assets. The threat that inside-user behaviour poses to the protection of information assets is therefore minimised.

The ISCF provides a comprehensive understanding of what information security culture comprises of. It therefore allows the researcher to use the components depicted in this framework to design an information security culture assessment instrument.

Research question 4: How does one conduct an assessment of information security culture?

An Information Security Culture Assessment process (ISCULA) is presented in Chapter 6. This process outlines what steps to follow to conduct an information security culture assessment in an organisation. It furthermore outlines how to design a valid assessment instrument based on an information security culture framework. It also portrays how to deploy the designed instrument and how to further test it to ensure that the assessment delivers valid and reliable results.

Chapter 7 discusses an empirical study of the assessment of information security culture by applying the ISCULA process. It illustrates how to validate an assessment instrument by ensuring that it is designed based on the ISCF and meets the statistical requirements for a valid and reliable assessment instrument. The process to conduct an information security culture assessment in an organisation is also illustrated by means of an empirical study highlighting the key steps to follow – from obtaining buy-in to providing recommendations to address the developmental areas identified in the assessment.

Research question 5: How does one provide valid and reliable results when assessing information security culture?

An information security culture assessment instrument is designed in Chapter 7. The dimensions assessed by the assessment instrument are based directly on the ISCF to ensure content validity. The validity of the assessment instrument is promoted as a theoretical foundation (the ISCF) is used to determine what to assess in terms of information security culture.

To further ensure valid and reliable results on which to base management decisions, the assessment instrument is statistically tested by using data from the empirical study. The validity of the assessment instrument is tested by considering acceptance criteria for which the minimum requirements were all met. The results indicate that the ISCF as theoretical framework can be accepted and that there is a good fit between the theoretical framework and the empirical data. The reliability of the assessment instrument is also confirmed, since all the statements met the minimum accepted criteria. This indicates that the statements made in the information security culture assessment instrument and the manner in which the statements are grouped can be accepted theoretically and statistically.

8.3 MAIN CONTRIBUTION

The main contribution of this research can be summarised as follows:

- An evaluation is conducted of the current research perspectives on the cultivation and assessment of information security culture. This provides a thorough understanding of the available perspectives and the contributions of each. The summary of the research perspectives helps the reader to understand the focus of each perspective and provides an overview of the research field at a specific point in time. It also highlights the need for further research on the cultivation and assessment of information security culture.

- The Comprehensive Information Security Framework, CISF, provides organisations with a holistic approach to the implementation of information security. Ultimately this framework provides management the means to implement an effective and comprehensive information security governance programme that addresses technical, procedural and people components. The framework provides a single point of reference for the governance of information security to inculcate an acceptable level of information security culture.
- The proposed ISCF furthermore considers all the components required for information security culture, namely information security, organisational culture and organisational behaviour. It integrates the aforementioned concepts to illustrate the influence between them. Because the information security components influence employees' information security behaviour, an information security culture is cultivated visibly as artifacts and creations, values and assumptions. The ISCF illustrates not only what information security culture is, but also how the information security culture is cultivated and can be directed through appropriate governance of the information security components. The ISCF further defines what one should assess in order to determine the level of information security culture in an organisation. It serves as the foundation for the design of a valid instrument to assess information security culture.
- An Information Security Culture Assessment process, ISCULA, is proposed. ISCULA is used to determine whether an acceptable level of information security culture is cultivated and if not, to deploy corrective action. ISCULA provides management with the steps to conduct an information security culture assessment, as well as the steps to validate the assessment instrument. When ISCULA is deployed in an organisation, it also has an influence on the information security culture. It raises awareness regarding the protection of information assets among the stakeholders involved as well as among employees responding to the questionnaire (assessment instrument). ISCULA therefore contributes to the cultivation of an information security culture.
- An information security culture assessment instrument is designed as part of the empirical study. This assessment instrument is designed using the

ISCULA process, thereby ensuring that it is valid and reliable from a theoretical as well as statistical perspective. This assessment instrument can be used in organisations to measure the prevailing information security culture. The results of the assessment help to identify areas of development in terms of the information security culture, and so help the organisation to take corrective action and achieve the desired level of information security culture.

- Ultimately this research helps to minimise the threats that user behaviour pose to the protection of an organisation's information assets. The ISCF facilitates the understanding of information security culture and shows how employee behaviour on various tiers could be directed through the governance of information security components in the organisation. Directing employee behaviour is further enabled through an assessment of users' attitude towards and perception of information security in the organisation. The results of the assessment can be used to direct the interaction of humans with computer information systems and so contribute to the protection of information assets.

8.4 LIMITATIONS

The current research study has the following limitations:

- Predictive or exploratory model: This research does not incorporate the development of a predictive or exploratory model that explains or predicts information security culture if employee behaviour is changed. Neither does it identify the possible behaviour outcomes for each component in the ISCF on each of the framework tiers. (For example, if employees read the information security policy would it improve their behaviour to be conducive to the protection of information assets and does it positively influence the information security culture?) Such a model would include hypotheses derived from theory and validate them by using indexes in terms of Structural Equation Modelling.
- Research method: The ISCULA process incorporates only a quantitative research method where information is gathered purely through a

questionnaire. Other methods such as focus groups and assessment centres are not incorporated.

- Assessment data: The information security culture assessment data used to validate the assessment instrument are obtained from one organisation only. The research study does not incorporate more than one survey's data nor does it extend to a second survey in the same organisation to enable to researcher to benchmark the data and identify whether the information security culture indeed improved after the implementation of action plans.
- Assessment instrument: The developed statements in the information security culture assessment instrument are not categorised to be answered by different audiences in an organisation. This could be useful as not all employees would for instance be in the position to answer the management and strategic questions.

8.5 FUTURE RESEARCH

The study achieved the objectives set out for this research, but has certain limitations that call for future research work to supplement and support the current findings, namely:

- Structural Equation Modelling can be deployed to develop an exploratory model for information security culture. Such a model can illustrate possible relationships and influences between components identified in the ISCF. The model can subsequently be compared with the theoretical framework and hypotheses to further improve both the ISCF and the assessment instrument. It could also provide better insight into the further interpretation of the assessment results and enable the reader to understand the relationships between the results of the different information security components being assessed.

  Possible behaviour outcomes for each component in the ISCF can be developed by using hypotheses and can be validated though Structural

Equation Modelling. This could illustrate the information security culture that should be evident as a result of the implementation of an information security component in a specific information security behavioural tier. For example, appointing an information security sponsor on the organisational level could result in commitment from management towards information security in general. Implementing an information security strategy together with a sponsor could lead to commitment from management to implement the security requirements, as they understand better what is expected of them. A behaviour outcome for management could be a positive perception and a commitment to motivate staff to comply with the information security policy. Without an information security strategy in place, management might feel positive towards information security, but will not communicate requirements to staff or implement security requirements in projects. In the absence of a sponsor, however, management might forget entirely about information security in their daily operations.

- ISCULA could be expanded to include a qualitative research perspective such as considering interviews, walk-abouts and even reviewing the information security policy.
- A second information security culture assessment should be conducted in the organisation where the empirical study was conducted. The results of the assessment conducted in this research should serve as the benchmark data against which to compare the second assessment. This will provide insight into whether the recommendations that were implemented as a result of the information security culture assessment had a positive influence on the information security culture of the organisation.
- Further information security culture assessments should be conducted to provide benchmark data across organisations. The results can be used to compare the level of information security culture across different industries, for instance financial organisations, energy and natural resource organisations and health care. The results could aid in understanding whether a lower level of protection of their information assets is acceptable to some industries within the context of their business operations compared to other industries.

- The information security culture assessment instrument can be further improved as it matures over time with application in organisations. The current set of information security culture statements can for instance be refined to be answered by specific audiences in the organisation. For example, a specific set of questions for management, another for the IT department, another for the Information Security Officer and another for general users. This could aid in providing more accurate results, as users only provide a useful opinion for statements that are applicable to them. For instance, a general user (as opposed to the Information Security Officer and sponsor) might not know how much is budgeted for information security or whether it is enough.
- The components of the ISCF should continually be revised and adapted to reflect current technological and governance requirements. Should the ISCF be adapted, the assessment instrument would also have to be revised accordingly and validated.

Bibliography

Albrechtsen, E. 2007. A qualitative study of users' views on information security. *Computers and Security*, 2007(26): 276-289.

Andress, M. 2000. Manage people to protect data. *InfoWorld*, 22(46): 48.

Andric, M. 2007. Fighting the enemy within. *IT WEB Special Report*, April 2007(95): 54.

Ashkanasy, N.M., Wilderom, C.P.M. & Peterson, M.F. (eds). 2000. *Handbook of organisational culture & climate.* California: Sage Publications.

Baggett, W.O. 2003. Creating a culture of security. *The Internal Auditor*, (60)3: 37-41.

Berry, M.L. & Houston, J.P. 1993. *Psychology at work.* Wisconsin: Brown and Benchmark Publishers.

Borking, J. 2006. Without privacy standards no trust in and outside cyberspace. Retrieved online on 25 April 2008 from https://www.prime-project.eu/events/standardisation-ws/slides/Withoutprivacynotrust-JohnBorking.pdf/file_view

Bresz, P.F. 2004. People – often the weakest link in security, but one of the best places to start. *Journal of Health Care Compliance*, (6)4: 57-60.

Brewerton, P. & Millward, L. 2002. *Organizational research methods*. London: Sage Publications.

BS 7799 (BS 7799-2). 2002. *Information technology*. Security techniques. Information security management systems – requirements.

Chau, P.Y.K. 1999. On the use of construct reliability in MIS research: a meta-analysis. *Information Management*, (35)4: 217-227.

Cardinali, R. 1995. Reinforcing our moral vision: Examining the relationship between unethical behaviour and computer crime. *Work Study*, 44(8): 11-18.

Church, A.H. & Waclawski, J. 1998. Organizational *surveys – a seven step approach*. San Francisco: Jossey-Bass.

CISA Review Manual. 2005. ISACA: Rolling Meadows.

COBIT security baseline – An information security survival kit. 2004. USA: IT Governance Institute.

Connolly, P.J. 2000. Security starts from within. *InfoWorld,* 22(28): 39-40.

Da Veiga, A., Martins, N. & Eloff, J.H.P. 2007. Information security culture – validation of an assessment instrument. *Southern Africa Business Review*, (11)1: 146-166.

Deloitte & Touche LLP, Ernst & Young LLP, KPMG LLP & PricewaterhouseCoopers LLP. 2004. Perspectives on Internal Control Reporting - a Resource for Financial Market Participants. Retrieved online on 18 January 2007 from http://www.ey.com/global/download.nsf/

Dervin, L., Kruger, H. & Steyn, T. 2006. Value-focused assessment of information communication and technology security awareness in an academic environment. **In** IFIP International Federation for Information Processing, *Security and Privacy in Dynamic Environments*, 201: 448-453.

Detert, J.R., Schroeder, R.G. & Mariel, J. 2000. A framework linking culture and improvement initiatives in organisations. *The Academy of Management Review*, 25(4): 850-863.

Dillon, W.R., Madden, J.T. & Firtle, N.H. 1993. *Essentials of marketing research*. Boston: IRWIN.

Dojkovski, S., Lichtenstein, S. & Warren, S. 2006. Fostering information security culture in small and medium size enterprises: An interpretive study in Australia. Retrieved online on 8 August 2007 from http://csrc.lse.ac.uk/asp/aspecis/20070041.pdf

Donaldson, W.H. 2005. U.S. Capital Markets in the Post-Sarbanes-Oxley World: Why Our Markets Should Matter to Foreign Issuers. Chairman, U.S. Securities and Exchange Commission. London School of Economics and Political Science.

Electronic Communications and Transactions Act (ECTA). 2002. Retrieved online on 12 January 2006 from http://www.acts.co.za/ect_act/

Eloff, J.H.P. & Eloff, M. 2005. Integrated Information Security Architecture, *Computer Fraud and Security*, 2005(11): 10-16.

Finance. 2008. Retrieved online on 22 August 2008 from www.finance.gov.au/gateway/guidance_glossary.html.

Flowerday, S. & Von Solms, R. 2006. *Trust an element of information security*. In *Security and Privacy in Dynamic Environments*. IFIP/SEC2005. Boston: Kluwer Academic Publishers, 87-97.

Furnell, S.M. 2004. Enemies within: the problem of insider attacks. *Computer Fraud & Security*. 2004(July): 6-11.

Furnell, S.M. 2007. IFIP workshop – Information security culture. *Computers and Security*, 2007(26): 35.

Furnham, A. & Gunter, B. 1993. *Corporate assessment: Auditing a company's personality*. London: Routledge.

Gaunt, N. 2000. Practical approaches to creating a security culture. *International Journal of Medical Informatics*, 60(2): 151-157.

Grant, R. 2005. Building a strong security culture. Retrieved online on 16 January 2006 from http://www.citec.com.au/news/featureNews/2005/April/security_culture.shtml?rate

Guldenmund, F.W. 2000. The nature of safety culture: A review of theory and research. *Safety Science*, 34: 215-257.

Hall, E.M. 1998. *Managing risk: Methods for software systems development.* Reading: Addison-Wesley.

Health Insurance Portability & Accountability Act. (HIPAA). 2006. Retrieved online on 1 August 2006 from http://www.asksam.com/ebooks/hipaa/

Helle, A.J. 2005. Security culture and risk management is a management responsibility. Retrieved online on 16 January 2006 from http://64.233.161.104/search?q=cache:iz7ehU05geYJ:www.telenor.com/telektronikk/volumes/pdf/1.2005/Page_011-014.pdf+information%2Bsecurity%2Bculture&hl=en

Hellriegel, D., Slocum, Jr. J.W. & Woodman, R.W. 1998. *Organizational behavior*. Eighth edition. South-Western College Publishing.

Helokunnas, T. & Kuusisto, R. 2003. Information Security Culture in a Value Net. In *2003 IEEE International Engineering Management Conference*, Albany, New York.

Helokunnas, T. & Ilvonen, I. 2004. Information security culture in small and medium sized enterprises. Retrieved online on 16 January 2006 from http://64.233.161.104/search?q=cache:BQkgIbn4EawJ:www.ebrc.info/kuvat/2034.pdf+information%2Bsecurity%2Bculture&hl=en

Hintze, J.L. 1997. Number Cruncher Statistical Systems, version 5.03 5/90. Kaysville, UT: NCSS.

Howell, D.C. 1995. Fundamental statistics for the behavioral sciences. 3rd International Standards Organisation. Retrieved online in January 2005 from http://www.iso.ch

Huysamen, G.K. 1988. *Sielkundige meting – 'n Inleiding*. Pretoria: J.L. van Schaik.

Information Security Forum. 2000. *Information Security Culture – A preliminary investigation.* s.l

Information Security Forum. 2003. *Standard of Good Practice for Information Security.* s.l.

Information Security Forum. 2008. Retrieved online on 11 February 2008 from www.securityforum.org

ISACA. 2008. Information Systems Audit and Control Association. http//:www.isaca.org

ISO/IEC 17799 (BS 7799-1). 2000. *Information technology. Security techniques. Code of practice for information security management.*

ISO/IEC 17799 (BS 7799-1). 2005. *Information technology. Security techniques. Code of practice for information security management*.

ISO/IEC 27001 (BS 7799-2). 2005. *Information technology. Security techniques. Information security management systems – requirements*.

King Report II. 2001. The King Report of corporate governance for South Africa. Retrieved online on 12 January 2006 from http://www.iodsa.co.za/downloads/King%20II%20Report%20CDRom%20Brochure.pdf

Kraemer, S. & Carayon, P. 2005. Computer and Information security culture – findings from two studies. **In** *Proceedings of the human factors and ergonomics society 49th annual meeting.* Retrieved online on 20 July 2007 from http://ecow.engr.wisc.edu/cgi-bin/get/ie/705/karsh/readings/hfesorland/kraemeruw-madison2005.pdf

Kraemer, S. & Carayon, P. 2007. Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists. *Applied Ergonomics*, 38(2007): 143-154.

Kraemer, S., Carayon, P. & Clem, J.F. 2006. Characterising violations in computer and information security systems. Retrieved online on 20 June 2007 from http://cqpi2.engr,wisc.edu/cis/docs/skiea2006.pdf.

Kraut, A.I. 1996. *Organizational Surveys*. San Francisco: Jossey-Bass Publishers.

Kreitner, R. & Kinicki, A. 1995*. Organizational behavior*. Chicago: IRWIN Inc.

Krejcie, R.V. & Daryle, M.W. 1970. Determining sample size for research activities. *Educational and Psychological Measurement, 1970(30): 607-610.*

Kruger, H.A. & Kearney, W.D. 2006. A prototype for assessing information security awareness. *Computers & Security*, 25(2006): 289-296.

Kuusisto, R. & Ilvonen, I. 2003. Information security culture in small and medium-sized enterprises. *Frontiers of E-business Research.* Retrieved online on 20 June 2007 from http://www.ebrc.fi/kuvat/431-439.pdf

Le Grand, C. & Ozier, W. 2000. Information Security Management Elements. Retrieved online on 20 March 2000
from http://www.itaudit.org/forum/auditcontrol/f305ac.htm

Lundy, O. & Cowling, A. 1996. *Strategic human resource management*. London: Routledge.

Magklaras, G.B. & Furnell, S.M. 2004. A preliminary model of end user sophistication for insider threat prediction in IT systems. *Computers & Security*, 25(2006):27-35.

Martins, A. 2002. *Information security culture*. Johannesburg: Rand Afrikaans University. (M.Com thesis.)

Martins, A. & Eloff, J.H.P. 2002. Information security culture. In *Security in the information society*. IFIP/SEC2002. Boston: Kluwer Academic Publishers: 203-214.

Martins, N. & von der Ohe, H. 2003. Organisational climate measurement – new and emerging dimensions during a period of transformation. *South African Journal of Labour Relations*, (27)3 and 4: 41-59.

McCarthy, M.P. & Campbell, S. 2001. *Security transformation*. New York: McGraw-Hill.

McHaney, R., Hightower, R. & Pearson, J. 2002. A validation of end-user computing satisfaction instrument in Taiwan. *Information Management*, (39)6: 503-511.

McIlwrath, A. 2006. *Information security and employee behaviour*. Hampshire: Gower.

NCSU. 2008. Retrieved online on 22 August 2008 from www.ncsu.edu/scrc/public/DEFINITIONS/G%20-%20I.html

Nosworthy, J.D. 2000. Implementing information security in the 21st century – do you have the balancing factors? *Computers and Security*, 19(4): 337-347.

Odendaal, A. 1997. *Deelnemende bestuur en korporatiewe kultuur: onafhanklike konstrukte? / Participative management and corporate culture: independent constructs?* Rand Afrikaans University: Johannesburg. (MA thesis.)

Olivier, M.S. 1999. *Information Technology Research – A practical guide.* Rand Afrikaans University: Johannesburg.

Pfleeger, C.P. 1997. *Security in computing*. Second edition. New Jersey: Prentice Hall.

Pocket Oxford Dictionary 1.0. 2005. Retrieved online on 1 January 2008 from http://freedownloadscentre.com/Palm_Pilot/Utilities/Pocket_Oxford_English_Dictionary.html

Posthumus, S. & Von Solms, R. 2005. IT Governance. *Computer Fraud and Security*, 2005(6): 11-17.

Puhakainen, P. 2006. A design theory for information security awareness. Retrieved online 31 July 2008 from http://herkules.oulu.fi/isbn9514281144/isbn9514281144.pdf.

PriceWaterhouseCoopers. Information security breaches survey. 2004. Retrieved online on 12 March 2005 from http://www.dti.gov.uk/industry_files/pdf/isbs_2004v3.pdf

Promotion of Access to Information Act (PROATIA). 2000. Retrieved online on 12 January 2006 from http://www.acts.co.za/prom_of_access_to_info/index.htm

Purser, S. 2004. Integrating security into the corporate culture. Retrieved online on 16 January 2006 from http://www.infosecwriters.com/texts.php?op=display&id=249

Rees, J., Bandyopadhyay, S. & Spafford, E. 2003. PFIRES: A policy framework for information security. *Communications of the ACM*, (46)7: 101-106.

Robbins, S.P. 1997. *Organizational behaviour*, 5th ed. New Jersey: Prentice Hall.

Robbins, S.P. 1998. *Organizational behaviour.* 8th ed. New Jersey: Prentice Hall.

Robbins, S. 2001. *Organizational behaviour*. 9th ed. New Jersey: Prentice Hall.

Robbins, S., Odendaal, A. & Roodt, G. 2003. *Organisational behaviour – Global and Southern African perspectives.* Pearson Education South Africa: Cape Town.

Ruighaver, A.B. & Maynard, S.B. 2006. Organisational security culture: More than just an end user phenomenon. **In** *IFIP International Federation for Information Processing*, Security and Privacy in Dynamic Environments, 201: 425-430.

Ruighaver, A.B., Maynard S.B. & Chang, S. 2006. Organisational security culture: Extending the end-user perspective. *Computers and Security,* 2007(26): 56-62.

Sartor, R. 2008. Privacy, reputation and trust: Some implications for data protection. Retrieved online on 25 April 2008 from http://www2.cirsfid.unibo.it/~sartor/GSCirsfidOnlineMaterials/GSOnLinePublications/GSPUB2006PrivacyReputationTrust.pdf

SAS. 2008. Statistical Analysis Software. Retrieved online on 31 July 2008 from http://www.sas.com/technologies/analytics/statistics/stat/index.html.

Schein, E.H. 1985. *Organizational culture and leadership.* San Francisco: Jossey-Bass Publishers.

Schermelleh-Engel, K., Moosbrugger, H. & Muller, H. 2003. Evaluating the fit of structural equation models: Test of significance and descriptive goodness-of-fit measures. *Methods of Psychological Research Online*. 8(2): 23-74.

Schiesser, R. 2002. *IT systems management*. Upper Saddle River: Prentice Hall.

Schlienger, T. 2006. *Informationssicherheitskultur in Theorie und Praxis: Analyse und Förderung sozio-kultureller Faktoren der Informationssicherheit in Organisationen.* iimt University Press: Fribourg. (Published D. Phil. thesis)

Schlienger, T. & Teufel, S. 2002. Information security culture. **In** *Security in the Information Society.* IFIP/SEC2002. Boston: Kluwer Academic Publishers: 191-201.

Schlienger, T. & Teufel, S. 2003a. Information security culture: from analysis to change. **In** *Information Security South Africa – Proceedings of ISSA 2003, 3rd Annual Information Security South Africa Conference*. South Africa. ISSA: 183-195

Schlienger, T. & Teufel, S. 2003b. Analysing information security culture: Increased trust by an appropriate information security culture. **In** *International Workshop on Trust and Privacy in Digital Business Trust Bus'03) in conjunction with 14th International Conference on Database and Expert Systems Applications (14th: 2003: Prague)*. Czech Republic.

Schlienger, T. & Teufel, S. 2005. Tool supported management of information security culture. **In** *IFIP International Information Security Conference (20th: 2005: Makuhari-Messe, Chiba)*. Japan.

Sherwood, J., Clark, A. & Lynas, D. 2005. *Enterprise security architecture. A business-driven approach.* CMP Books: Berkeley.

Siponen, M., Pahnila, S. & Mahmood, A. 2007. Employees' adherence to information security policies: An empirical study. **In** *Proceedings of New*

Approaches to Security, Privacy and Trust in Complex Environments, FIP/SEC2007, Sandton, South Africa: 133-144.

SSE-CMM. 2008. Systems Security Engineering Capability Maturity Model. Retrieved online on 31 July 2008 from http://www.sse-cmm.org/index.html

Standard of Good Practice. 2003. Information Security. Information Security Forum. Retrieved online on 20 February 2008 from https://www.securityforum.org/html/frameset.html

Stanton, J.M., Stam, K.R., Mastrangelo, P. & Jolton, J. 2005. Analysis of end user security behaviours. *Computers and Security*, (24)2: 124-133.

Starnes, R. 2006. Creating a security culture. Retrieved online on 16 January 2006 from http://www.cw.com/uk/solutions/business/risk_security/story_0501004_starnes.html

Stewart, J.N. 2006. CSO to CSO: Establishing the security culture begins at the top. Retrieved online on 16 January 2006 from http://cisco.com/web/about/security/intelligence/05_07_security-culture.html

Straub, D. 1989. Validating instruments in MIS research. *MIS Quarterly*, (13)2: 147-169.

Straub, D.W. 1990, Effective IS security: an empirical study. *Information Systems Research*, (1)3: 255-276.

Straub, D., Boudreau, M. & Gefen, D. 2004. Validation guidelines for IS positivist research, *Communications of the Association for Information Systems*, (13)24: 380-427.

Survey Tracker. 2008. Retrieved online on 23 January 2008 from http://www.surveytracker.com

Tessem, M.H. & Skaraas, K.R. 2005. Creating a security culture. Retrieved online on 16 January 2006 from http://www.telenor.com/telektronikk/volumes/pdf/1.2005/Page_015-022.pdf

The Concise Oxford Dictionary. 1983. Oxford: Clarendon Press.

The promotion of a culture of security for information systems and networks in OECD countries (OECD), DSTI/ICCP/REG(2005)1/FINAL.2005. Retrieved online on 8 August 2006 from http://www.oecd.org/document/42/0,2340,en_2649_34255_15582250_1_1_1_1,00.html

Thomson, I. 2004. IT security culture must start from the top – Global survey warns senior execs against 'delegating' security awareness. Retrieved online

on 16 January 2006 from
http://www.vnunet.com/vnunet/news/2125904/security-culture-start-top

Thomson, K. & Von Solms, R. 2005. Information security obedience: a definition. *Computers and Security*, 2005(24): 69-75.

Thomson, K., Van Solms, R. & Louw, L. 2006. Cultivating an organisational information security culture. *Computer Fraud and Security,* October (2006): 7-11.

Thomson, K. & Von Solms, R. 2006. Towards an information security competence maturity model. *Computer Fraud and Security*, 2005(5): 11- 14.

Trček, D. 2003. An integral framework for information systems security management. *Computers and Security*, 22(4): 337-360.

Trompeter, C.M. & Eloff, J.H.P. 2001. A framework for the implementation of socio-ethical controls in Information Security. *Computers and Security*, 20(5): 384-391.

Tudor, J.K. 2000. *Information Security Architecture – An integrated approach to security in an organisation*. London: Auerbach.

Tudor, J.K. 2006. *Information security architecture - An integrated approach to security in organisations*. Boca Raton: Auerbach.

Van der Merwe, P. & Cantale, S. 2007. Cyber-baddies make jay as CIOs snooze. *Brainstorm*, 6(9): 59-66.

Van der Raadt, B., Soetendal, J., Perdeck, M. & Van Vliet, K. 2004. Polyphony in architecture. **In** *Proceedings of the 26th International Conference on Software Engineering (ICSE'04).* IEEE.

Van Niekerk, J. & Von Solms, R. 2005. An holistic framework for the fostering of an information security sub-culture in organizations. **In** *Information Security South Africa – Proceedings of ISSA 2005, 4th Annual Information Security South Africa Conference. South Africa.* Retrieved online on 16 March 2008 from http://icsa.cs.up.ac.za/issa/2005/Proceedings/Full/041_Article.pdf

Van Niekerk, J. & Von Solms. R. 2006. Understanding information security culture: A conceptual framework. **In** *Information Security South Africa – Proceedings of ISSA 2006, 5th Annual Information Security South Africa Conference. South Africa.* Retrieved online on 16 March 2008 from http://icsa.cs.up.ac.za/issa/2006/Proceedings/Full/21_Paper.pdf

Verton, D. 2000. Companies aim to build security awareness. *Computerworld,* 34(48): 24.

Von Solms, B. 2000. Information security – The third wave? *Computers and Security,* 19(7): 615-620.

Von Solms, B. 2005. Information security governance – compliance management versus operational management. *Computers and Security*, (24)6: 443-447.

Von Solms, B. 2006. Information security – The fourth wave. *Computers and Security*, 25(2006): 165-168.

Von Solms, R. & Von Solms, B. 2003. From policies to culture. *Computers and Security,* (2004)23: 275-279.

Von Solms, R. 1998. Information security management (3): The code of practice for information security management (BS7799). *Information Management and Computer Security,* 6(5): 224-225.

Vroom, C. & Von Solms, R. 2004. Towards information security behavioural compliance. *Computers and Security,* (23)3: 191-198.

Walters, M. 1996. *Employee attitude and opinion surveys*. London: Institute of Personnel and Development.

Walton CB, R., & Walton-Mackenzie Limited. 2006. Balancing the insider and outsider threat. *Computer Fraud and Security*, 2006(11): 8-11.

Whitman, M.E. & Mattord, H.K. 2003. *Principles of information security.* Kennesaw State University: Thomson Course Technology.

Willison, R. & Siponen, M. 2007. A critical assessment of IS security research between 1990-2004. **In** *Proceedings of the 15th European Conference of Information Systems,* St. Gallen, Switzerland, June 7-9, 2007.

Witty, R.J. & Hallawell, A. 2003. Client issues for security policies and architecture. Gartner. ID number: K-20-7780.

Woon, I.M.Y., Tan, G.W. & Low, R.T. 2005. A protection motivation theory approach to home wireless security. **In** *Proceedings of the twenty-sixth International Conference on Information Systems*, Las Vegas, 367-380.

Workman, M., Bommer, W.H. & Straub, D. 2008. Security lapses and the omission of information security measures: A threat control model and empirical test, *Computers in Human Behaviour*, Article in press – corrected proof. Retrieved online on 31 July 2008 from http://www.sciencedirect.com.

Yang, Z., Cai, S., Zhou, Z. & Zhou, N. 2005. Development and validation of an instrument to measure user perceived service quality of information presenting web portals. *Information & Management*, (42)4: 575-589.

Zachman, J. 2008. *Zachman framework*. Retrieved online on 8 February 2008 from http://www.zifa.com/

Zakaria, O. 2006. Internalisation of information security culture amongst employees through basis security knowledge. **In** *IFIP International Federation for Information Processing,* Security and Privacy in Dynamic Environments. Fisher-Hübner, S., Rannenberg, K., Yngström L. & Lindskog, S. (eds). 201: 437-441.

Zakaria, O. & Gani, A. 2003. A conceptual checklist of information security culture. **In** *Proceedings of the 2nd European Conference on Information Warfare and Security*, Reading, UK.

APPENDICES

APPENDIX A – INFORMATION SECURITY CULTURE ASSESSMENT INSTRUMENT

APPENDIX B – INITIAL INFORMATION SECURITY CULTURE ASSESSMENT INSTRUMENT (DA VEIGA, MARTINS & ELOFF, 2007)

APPENDIX C – INFORMATION SECURITY CULTURE ASSESSMENT REPORT

APPENDIX D – PAPER PUBLISHED IN JOURNAL: INFORMATION SECURITY CULTURE – VALIDATION OF AN ASSESSMENT INSTRUMENT

Information security culture – validation of an assessment instrument

A. da Veiga, N. Martins & J.H.P. Eloff

ABSTRACT

Organisations need to ensure that the interaction among people, as well as between people and information technology (IT) systems, contributes to the protection of information assets. Organisations therefore need to assess their employees' behaviour and attitudes towards the protection of information assets in order to establish whether employee behaviour is an asset or a threat to the protection of information. One approach that organisations could use is to assess whether an acceptable level of information security culture has been inculcated in the organisation and, if not, take corrective action. The aim of this paper is to validate an information security culture assessment instrument. This is achieved by performing a factor and reliability analysis on the data from an information security culture assessment in a financial organisation. The results of the analysis are used to identify areas for improving the information security culture assessment instrument. The study makes a contribution to the existing body of knowledge concerned with the assessment of information security culture and its value for management to ensure the protection of information assets.

Key words: information security, information security culture, information security awareness, behaviour, measure, assess, questionnaire, validity, reliability, survey

INTRODUCTION

Information security encompasses technology, processes and people (Von Solms 2000; Tessem & Skaraas 2005). It comprises a suitable set of controls such as organisational structures, software principles and e-mail practices implemented by the organisation. These information security controls are implemented to ensure the confidentiality,

Ms A. da Veiga and Prof. J.H.P. Eloff are in the Information and Computer Security Architectures Research Group, Department of Computer Science, University of Pretoria. Prof. N. Martins is in the Department of Industrial Psychology, University of South Africa. E-mail: adele.daveiga@kpmg.co.za

integrity and availability of the organisation's information, which may be essential to maintaining a competitive edge, cash flow, profitability or legal compliance (ISO 2005).

Many organisations are at the stage where they have implemented technology and compiled information security policies and procedures to protect the organisation's information from a wide variety of threats. These threats could vary from computer-assisted fraud, espionage, sabotage and vandalism to fire. According to the Control Objectives for Information and related Technology (COBIT) Security Baseline Survival Kit (COBIT 2004), a lack of security awareness could cause a gap in an organisation's implementation of information security. Organisations now have to ensure that employees are aware of their responsibility in securing information assets such as archived information, system documentation, business strategies and databases (COBIT 2004; ISO 2005). Employees must also be adequately trained in order for the organisation to direct their behaviour to minimise accidental and malicious threats to information assets. The ISO17799 (ISO 2005) standard states that "providing appropriate training, education and awareness" is critical to the successful implementation of information security. It is therefore important that the members of an organisation's workforce are aware and conscious of information security in their daily work activities. In each organisation, an information security culture will emerge over time and become evident in the behaviour and activities of the workforce. This information security culture that develops can be defined as the assumption about those perceptions and attitudes that are accepted and encouraged in order to incorporate information security characteristics as the way in which things are done in an organisation, with the aim of protecting information assets (Martins & Eloff 2002; Martins 2002). For organisations to manage security risks to information assets, they must have a strong information security culture (Baggett 2003; CITEC 2005; Dervin, Kruger & Steyn 2006; Gaunt 2000; ISF 2000; Martins & Eloff 2002; Ruighaver & Maynard 2006; OECD 2005; Stewart 2006; Schlienger & Teufel 2005; Tessem & Skaraas 2005; Thomson 2004; Von Solms 2006; Zakaria 2006).

Various factors motivate the importance of inculcating an information security culture in order to protect the information assets of organisations. The people who are expected to be responsible for information security constitute one of the main factors in this equation. Research illustrates that the interaction of people and the behaviour of employees towards computer and information assets represent the weakest link in information security (Abu-Musa 2003; Baggett 2003; Bresz 2004; Martins & Eloff 2002; Schlienger & Teufel 2002).

Based on a survey conducted by PricewaterhouseCoopers in 2004 (PWC 2004), a comparison was made between various surveys to illustrate the number of organisations that had experienced a security incident. As many as 83% of respondents indicated that they had experienced high-technology information security incidents. The three most common breaches were virus infections, staff

misuse of the Internet and physical theft of computer equipment. Although the number of technology incidents was very high, the report stated that "human error rather than technology is the root cause of most security breaches" (PWC 2004). According to PricewaterhouseCoopers, the solution would be to create a security-aware culture. Staff should be made more aware of the risks and of their responsibilities, thereby enabling them to act in a sensible and secure manner. The Guidelines for Security of Information Systems and Networks (Baggett 2003; OECD 2005) of the Organisation for Economic Cooperation and Development (OECD) provide a comprehensive framework for creating a culture of security. Through principles such as awareness, responsibility and ethics, a security culture will begin to develop – thereby minimising the threat that users pose to computer assets.

The organisation thus needs to ensure that an information security culture is inculcated through training, education and awareness in order to minimise risks to information assets. To determine whether the information security culture is at an acceptable level, it needs to be measured and reported on. One way of measuring the level of an organisation's information security culture is to use an information security culture assessment instrument (questionnaire) (Martins & Eloff 2002; Martins 2002; Schlienger & Teufel 2005). The results obtained from such an assessment can be used to identify areas for improving the protection of information assets.

AIM OF THIS PAPER

The aim of this paper is to validate an assessment instrument for assessing information security culture and provide one that is accepted as a valid and reliable assessment instrument in the information security and psychology research fields. In order to achieve the aim of the paper, an information security culture assessment was conducted in a financial organisation using an information security culture questionnaire.

CURRENT DEVELOPMENTS IN INFORMATION SECURITY CULTURE ASSESSMENTS

Perspective of the Information Security Forum

During November 2000, the Information Security Forum (ISF 2000) released a report discussing the definition of information security culture and the factors on which to focus when measuring it. They started their research in the realisation that despite compelling evidence that well-directed action can reduce information risks, incidents continue to occur on a daily basis. They concluded that this was probably due to a lack of a strong information security culture for driving down risk.

Based on the research work that the ISF conducted, they propose to develop a questionnaire to measure information security culture (ISF 2000). The main objective of the questionnaire would be for an organisation to identify the effect of information security culture on the organisation's level of information risk and specific target areas for improvement. As part of the ISF's future work, they plan to pilot the questionnaire at member firms, standardise it, enable benchmarking between organisations, and develop an implementation guide for organisations to use the measurement tool (ISF 2000).

Perspective of Schlienger and Teufel

Schlienger & Teufel (2002) introduced a paradigm shift – from a technical approach, towards information security, to a socio-cultural approach. They concluded that one has to focus on the organisational culture in addressing the human element so as to minimise risks to information assets and concentrate on the information security culture of the organisation.

Schlienger & Teufel (2003; 2005) selected the survey method, using a questionnaire, to obtain an understanding of the official rules that are supposed to influence the security behaviour of employees. Schlienger & Teufel's (2005) questionnaire takes into account the three levels of organisational behaviour of Robbins (2001), as well as research work performed by Schein (1985). It measures 20 areas (for example, leadership, problem management, communication and attitude). They performed substantive research to develop a decision-support system for analysing the results automatically and enabling employees to complete the questionnaire online. This tool was implemented in a private bank, and the application illustrated its usefulness. The Working Group on Information Security Culture of the Information Security Society of Switzerland (FGSec) also participated through discussions to ensure the practicability of the process. Schlienger & Teufel further aim to focus on extending the tool to allow benchmarking (Schlienger & Teufel 2005).

Perspective of Martins and Eloff

Martins and Eloff (Martins 2002; Martins & Eloff 2002) designed an information security culture model based on the concepts of organisational behaviour (Robbins, Odendaal & Roodt 2003) and what constitutes information security. They identified information security controls at the individual, group and organisational levels of organisational behaviour that could influence information security culture (Martins 2002; Martins & Eloff 2002). This theoretical perspective provided the basis for the information security culture questionnaire and the items developed by the researchers to assess information security culture (Martins 2002; Martins & Eloff 2002). The

information security culture questionnaire, however, still needs to be statistically standardised through a large enough sample so as to provide data that can be used to conduct a factor and reliability analysis that will ensure its validity and reliability.

MEASURING INSTRUMENT

The purpose of this paper is to validate the assessment instrument developed by Martins & Eloff (2002) and Martins (2002). The information security culture questionnaire developed by Martins & Eloff was selected, as it is based on an information security culture model addressing content validity (Brewerton & Millward 2001); moreover, its usefulness and practicality had already been proven in a case study (Martins 2002, Martins & Eloff 2002). This questionnaire was developed for use in environments where awareness programmes had already been implemented, as well as those where such programmes had not previously been implemented. It could therefore be applied in financial organisations, even if they had not implemented any awareness programmes. In addition, the information security culture questionnaire includes knowledge questions that are analysed separately from the information security culture statements. These questions assess awareness of employees pertaining to information security requirements that management expects employees to know. The knowledge questions can be used to obtain information pertaining to current knowledge of employees that could result in specific behaviour. If an employee does not know what an information security incident is, one could argue that he/she will not effectively report such incidents. This contributes to the practicability of the questionnaire, as the financial organisation specifically required the knowledge questions to determine how much employees know about information security in order for management to determine what principles to include in the first awareness programme.

The financial organisation also required specific information in terms of ethical conduct, trust and change management. This information was necessary to aid management in tailoring their awareness programme to address any concerns in these areas. For instance, if management trusts its employees and the employees trust management, it is easier to implement new procedures and guide employees through changes of behaviour regarding information security. The perceptions of employees and management with respect to mutual trust need to be positive and should be regarded as a characteristic of the organisation that will aid in cultivating an information security culture from within. The information security culture questionnaire of Martins & Eloff focuses on these aspects and was found to be applicable to the requirements of the financial organisation. Apart from the data required by the researchers for the factor and reliability analysis, the financial organisation required the results of the survey for input to its awareness programme.

The information security culture questionnaire is divided into the following three sections (Martins 2002): (1) information security culture statements, (2) knowledge questions and (3) biographical questions.

Information security culture statements

This section assesses the perceptions of employees about eight different dimensions of information security: policies, management, programme, leadership, asset management, user management, change management and trust. A Likert scale (strongly agree, agree, unsure, disagree and strongly disagree) is used to answer the statements.

The following list reflects the statements in the information security asset management dimension:

- The organisation protects its information assets adequately (for example, systems and information).
- It is important to understand the threats to the information assets (for example, systems and information) in my department.
- Threats to security of information assets (for example, information and systems) are controlled adequately in my department.
- Information security is necessary in my department.
- The information assets (for example, systems and information) I work with need to be secured, either physically or electronically.
- I believe my business unit will survive if there is a disaster resulting in the loss of systems, people and/or premises.
- I feel safe in the environment I work in.
- I believe that the information I work with is adequately protected.

Knowledge questions

A section of knowledge questions is included to determine how much knowledge employees have about information security, and whether a low information security culture results from an educational problem or from perceptual concerns. A 'Yes/No' scale is used to answer these questions. The following five examples of knowledge questions are included in the information security culture questionnaire:

- The organisation has a written information security policy.
- I have read the information security policy sections that are applicable to my job.
- I know where to get a copy of the information security policy.
- I know what information security is.
- I know what an information security incident is.

Biographical questions

Biographical questions are included in the information security culture questionnaire in order to segment the data and draw comparisons within the population, for instance with regard to job levels or departments, as indicated by the following question:

What is your job level?

- Executive and senior managers
- Department managers and supervisors
- Operational staff (administrative, clerical, sales, etc.)
- Technology staff.

SURVEY METHODOLOGY

The survey methodology serves as a method that organisations can use to study information security behavioural content in general, as well as the attitude and opinions (Berry & Houston 1993) of employees with respect to information security in particular. This method is used to systematically gather data from members of an organisation for a specific purpose (Kraut 1996).

The process of designing, implementing, administering and reporting back on survey data is key to the success of the survey and perhaps even more important than the actual results generated (Kraut 1996). According to Berry & Houston (1993) and Kraut (1996), the main phases of a survey methodology should include planning and preparation, survey administration, data analysis, report writing and feedback to management and employees. Planning and preparation involve the participation of stakeholders, the customisation of the questionnaire, decisions on the population and sample size and a pilot study (Berry & Houston 1993; Church & Waclawski 1998). During the administration of the survey, the survey is communicated to the population and responses are monitored. The data are then statistically analysed, whereafter the report is compiled and feedback sessions are held to discuss action plans (Church & Waclawski 1998).

The following section discusses the survey methodology by illustrating how it was implemented in the financial organisation in order to obtain the data required for the factor and reliability analysis.

Planning and preparation

The first step in conducting a survey is to plan it (Berry & Houston 1993). The information security culture survey in the financial organisation was initiated through a formal project introduction meeting to obtain buy-in from relevant stakeholders and to discuss the project plan of operations (Berry & Houston 1993). As part of this meeting, the concept of information security culture was discussed, as well as the

approach that would be followed in conducting the survey. The stakeholders involved consisted of representatives from various departments – IT, information security, governance, risk management, human resources and training. The project sponsor was the Information Security Officer (ISO), and the various stakeholders assisted with the survey communication, technology set-up and coordination of the project across the target population to ensure that the required responses were obtained.

The second step was to conduct a workshop with the organisation's project team so as to customise the questionnaire (Berry & Houston 1993) developed by Martins (2002). IT as well as business representatives participated. Organisation-specific terminology was added to the information security culture questionnaire statements. The knowledge section of the information security culture questionnaire was also adjusted to incorporate questions specific to the environment of the organisation and any security awareness initiatives undertaken in the past. For instance, since the organisation has not rolled out an information security awareness programme in the past, no questions pertaining to such a programme were asked. The biographical questions were finalised based on the selected target population. These questions covered the business areas, geographical areas, length of service and job levels with respect to the organisation. It was decided that the information security culture questionnaire would be sent out to all employees in the selected business areas, altogether 12 572 employees. This method is referred to as convenience sampling (Brewton & Millward 2001).

Before the information security culture questionnaire could be rolled out to the target population, it had to be pretested on a small sample of employees to allow the researcher to understand the anticipated reactions of the larger group and to revise or restructure questions where necessary (Berry & Houston 1993). A group of 20 employees in the organisation completed the pilot survey in order to test the face validity of the information security culture questionnaire. Face validity is concerned with whether the questionnaire assesses what it says it does on the 'face of it' (Furnham & Gunter 1993). Minor adjustments were made to some of the culture statements to ensure that all employees would interpret the statements in the same manner. For instance, examples were added to some terms, and the word 'department' was changed to 'business area' as indicated in the box.

> My *business area* protects its information assets adequately *(e.g. systems and information in electronic or paper format)*.

The survey tool, Survey Tracker (2005), was used as the survey software to distribute, capture and conduct the survey analysis (Berry & Houston 1993). The information security culture questionnaire that was signed-off by the ISO had been designed in HTML format in Survey Tracker according to the scientific rules of

scales and question types built into the software. In collaboration with the IT department, a link to the information security culture questionnaire was added to the organisation's Intranet site, where employees could complete it. Figure 1 is an example of two statements extracted from the HTML-designed information security culture questionnaire.

	Strongly disagree	Disagree	Uncertain	Agree	Strongly agree
14. Information security should be part of key performance measures for the employees of the Group	•	•	•	•	•
15. Employees should be monitored on their compliance to information security policies and procedures (e.g. measuring the use of e-mail, monitoring which sites an individual visits or what software is installed on personal computes).	•	•	•	•	•

Figure 1: Extract from information security culture questionnaire

Survey administration

Communicating the survey and its objectives to employees is crucial in order to enhance the response rate and the quality thereof (Dillon, Madden & Firtle 1993). If questions are of a sensitive nature, and employees wish to remain anonymous, the organisation must ensure that individual responses cannot be identified (Berry & Houston 1993). For the purpose of this survey, the responses of the completed information security culture questionnaires were automatically saved in a file on one of the organisation's secure servers.

A communication e-mail was sent out to all employees from the 'Communication' mailbox a week before the survey was launched to prepare them for and inform them of the forthcoming survey. The survey ran for four weeks, during which employees were continually encouraged to complete the information security culture questionnaire online.

During this period, the responses were tracked to ensure that a statistically representative response was obtained for each biographical area into which the data would be segmented. Table 1 provides a summary of the divisions of the organisation, the number of employees in each, the statistically representative sample required and the actual response obtained. The method designed by Krejcie & Daryle (1970) was used to determine the required sample size. In only four divisions was this not representative. Trends were considered for these divisions.

When a validity test is conducted, the commonly accepted criterion is to have at least 100 respondents, or five times the number of responses compared to the number

of questions in the questionnaire (Martins 2000). The more accepted criterion is to have at least ten times the number of responses. This will ensure that the conclusions drawn from the sample data are not sample specific and that it is possible to generalise the findings (Martins 2000). The information security culture questionnaire consists of 42 statements that were used in the factor and reliability analysis. Overall, a representative number of 4 735 employees participated in the survey, which was a more than adequate sample.

Table 1: Information security culture questionnaire – representative sample

Division/ Business unit	Total number of employees	Sample required based on Krejcie & Daryle method	Actual responses	Representative (Yes/No)
Division A	1 847	318	1 213	Yes
Division B	261	155	160	Yes
Division C	1 146	217	500	Yes
Division D	132	75	93	Yes
Division E	3 481	346	675	Yes
Division F	668	191	381	Yes
Division G	1 311	224	536	Yes
Division H	311	172	124	No
Division I	660	245	209	No
Division J	72	61	42	No
Division K	77	64	40	No
Division L	2 606	335	545	Yes
Division M	No data	No data	144	No data
No response	n/a	n/a	73	n/a
Overall	12 572	355	4 735	Yes

Statistical analysis and results of the survey

The survey results were analysed using Survey Tracker (2005). Figure 2 shows the job levels of respondents. The respondents represented all job levels in the organisation: executive and senior managers (3.97%), department managers and supervisors (21.94%), operational job staff (64.16%) and technology staff (8.51%). Most respondents had worked for the organisation for more than ten years (32.06%) or for between 5 and ten years (23.59%), 77.4% worked at head office, and the rest at

branch offices. Responses were received from all nine provinces in South Africa, with the majority from Gauteng (62.09%), followed by the Western Cape (12.61%) and KwaZulu Natal (9.17%).

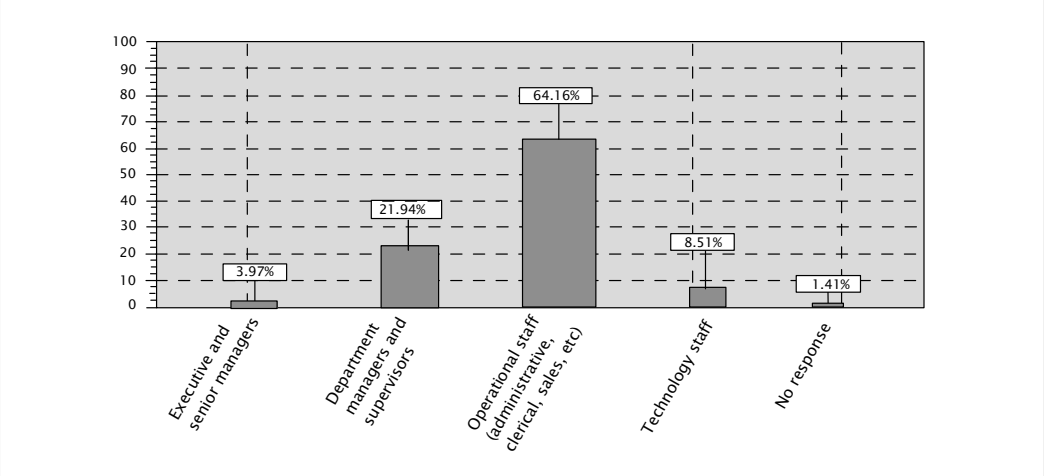


Figure 2: Job levels of respondents

Figure 3 shows the results of three of the knowledge questions as an example. The first column lists the question, the second provides the number of people that responded to the question, and the last column gives the percentage of people that answered 'Yes'. The figure illustrates that only 70.2% of the 4 691 respondents that answered the last question know where to get a copy of the information security policy. This would indicate that the organisation needs to communicate to employees where to obtain a copy of the information security policy and to ensure that the policy is kept or saved in a location where it is easy for employees to access it.

Statements	Count	Percentages of 'Yes' responses 0 20 40 60 80 100
The organisation has a written information security policy.	4 584	94.9%
I know what information security is.	4 690	92.2%
I know where to get a copy of the information security policy.	4 691	70.2%

Figure 3: Knowledge statement results

This concludes the discussion pertaining to the survey methodology used to conduct the information security culture assessment in the financial organisation in order to obtain data that could be used to validate the information security culture questionnaire.

FACTOR AND RELIABILITY ANALYSIS

The concept of validity implies that the researcher must ensure that the questionnaire assesses what it claims to assess (Berry & Houston 1993; Dillon, Madden & Firtle 1993; Furnham & Gunter 1993). Over time, such a questionnaire will yield reliable and stable results that prove to be valid (Dillon, Madden & Firtle 1993). Construct validity is considered for the validity analysis of the information security culture questionnaire. Construct validity is established using the principle components factor analysis to assess the robustness of the questionnaire dimensions, thereby identifying clusters of questions (statements) and forming new dimensions (Brewerton & Millward 2001). In the industrial psychology literature and in research, factor analysis is frequently used to assess whether instruments (questionnaires) measure substantive constructs which in this case are the nine dimensions of the information security culture questionnaire. Factor analysis as a statistical technique is employed to determine or uncover any underlying 'structure' that may exist in a data set (Brewton & Millward 2001; Howell 1995). It has various applications, which include establishing the structure of 'traits' that underlie personality, understanding the relationship between various performance criteria, and exploring the relationship between established work-related constructs (for example, leadership, communication, governance, awareness) (Brewton & Millward 2001; Martins & Von der Ohe 2003).

The principal components factor analysis (PCA) is a data analysis tool that is generally used to reduce the dimensionality (number of questions or statements) of a large number of interrelated questions, while retaining as much of the information (variation) as possible (Hintze 1997). The Number Cruncher Statistical Software (NCSS) program (Hintze 1997) was used for this purpose.

The latent root criterion (Hair, Anderson, Tatham & Black 1995), which specifies that all factors with eigenvalues of 1.00 or greater should be retained, was used. The eigenvalues are helpful in determining the variance of each factor and thus how many factors should be retained. The use of the eigenvalue as a cut-off point is possibly the most reliable criterion in determining how many factors to retain. All factors with a factor value greater than 1.00 were retained (Hintze 1997).

An initial factor extraction was done according to PCA, and the inter-correlation matrix was rotated according to the varimax method using the NCSS tool. The varimax method is used to obtain new factors or dimensions that are each highly correlated with only a few of the original variables (Hintze 1997).

Next, the reliability of each factor was determined by means of an item analysis (Cronbach alpha) that examines the correlation between each item and the scale total within a sample (Brewerton & Millward 2001). An item analysis is used to examine the frequencies and descriptive statistics for each item on the survey across all responses obtained (Church & Waclawski 1998). Reliability testing (Brewerton &

Millward 2001) is concerned with the degree of data consistency across a defined dimension. The purpose of both these techniques is to determine the reliability of an instrument (questionnaire). Both techniques were employed to assess whether the security culture instrument measures the substantive constructs (dimensions) and to test the reliability thereof.

DISCUSSION

The variance rotation isolated four factors, as listed in Table 2, which could be used as the four new information security culture dimensions and which accounted for 53.3% of the variance. According to Hintze (1997), factors that account for at least 50% of the variance are accepted. The interpretation of the factor matrix showed that none of the statements had a factor loading lower than 0.30, which is regarded as the cut-off point. According to Hair et al. (1995) a factor loading above 0.30 is regarded as meaningful and can be included in the dimensions. The internal consistency of the four new dimensions varies between 0.955795 and 0.676533 (Table 3). According to Brewton & Millward (2001), internal reliabilities between 0.6 and 0.7 are generally accepted as an absolute minimum to be identified as a factor.

Table 2: Results of initial factor analysis

Factor	Statement numbers
Factor 1	14, 15, 16, 22, 25*, 26, 28, 30, 33, 35, 38, 39, 40, 41, 42, 43, 44, 46, 47, 48, 49, 51, 52, 53
Factor 2	12, 17, 21, 23, 24, 25, 27, 28, 29, 31, 34, 36, 37
Factor 3	13, 18, 19, 22
Factor 4	45, 49, 50

* Item 25 loads high on factors 1 and 2

Table 3: Reliability analyses of initial analysis

Factors	Cronbach alpha	Number of items/ statements	Comments
Factor 1	0.955795	24	Item 25 loads high on factors 1 and 2
Factor 2: Management of information security	0.890352	16	
Factor 3: Performance management	0.677747	4	Item 22 loads high on factors 1 and 3
Factor 4: Performance accountability	0.676533	3	

A second-phase factor analysis was conducted for factor 1 in order to determine whether sub-dimensions could be formed. The same techniques and criteria were used as with the first analysis. The factors and factor loadings are presented in Tables 4 and 5. The factor loadings range between 0.807570 and 0.933200.

Table 4: Results of the factor analysis for the second-phase analysis – Factor 1

Factor	Statement numbers
Factor 5: Communication	22, 33, 35
Factor 6: Governance	14, 15, 16, 20, 25, 26, 30
Factor 7: Capability development	38, 39, 40, 41, 42, 43, 44, 46, 47, 48, 49, 51, 52, 53

Table 5: Reliability analysis of second-phase analysis

Factors	Cronbach Alpha	Number of items
Factor 5: Communication	0.807570	3
Factor 6: Governance	0.891884	7
Factor 7: Capability development	0.933200	14

Naming of factors

Conceptual naming of factors 2 to 7 was done after detailed inspection of the individual items (statements). The purpose was to attach a dimension name to each factor to make it understandable and identifiable for the information security culture questionnaire. Each of the new information security culture dimensions will next be discussed briefly.

Management of information security (factor 2)

This dimension includes the applicability of the information security policy, the understanding of threats to information assets, a willingness to change working practices to ensure the security of information assets and an acceptance of a responsibility towards information security.

Performance management (factor 3)

The items included in this dimension determine whether information security should be part of key performance measures, whether employees believe that they should be monitored, and whether the contents of the information security policy had been effectively explained to them, thus enabling employees to adhere to the policy.

Performance accountability (factor 4)

This dimension focuses on aspects such as whether action should be taken against people that do not adhere to the information security policy, whether employees feel safe where they work and whether people should be held accountable for their actions if they do not adhere to the information security policy.

Communication (factor 5)

The items included in this dimension focus on aspects such as the explanation of the information security policy, informing employees in a timely manner how information security changes will affect them, and informing people about what is expected of them regarding information security.

Governance (factor 6)

This factor focuses on aspects such as whether management adheres to the information security policy, the adequate protection of information assets, the perception of the importance of information security, and adequate control over information security assets.

Capability development (factor 7)

This dimension focuses on a number of aspects relating to employee trust, the commitment of time to information security, adherence to the information security policy by the various business areas, commitment to the policy and a belief that information is adequately protected.

This questionnaire with the six revised dimensions is hereafter referred to as the Information Security Culture Assessment (ISCA) questionnaire. Table 6 details the eight dimensions of the original information security culture questionnaire compared with the six new dimensions of the ISCA, as well as the number of statements per dimension. The six new dimensions have been constructed on the basis of the factor and reliability analysis as discussed, thereby ensuring that the new information security culture questionnaire meets the requirements for a reliable questionnaire as accepted in the statistical field.

After an analysis had been conducted of each of the items (statements) in the six ISCA dimensions, the items were regrouped and applicable names were given to each group of items relating to a single concept. The individual statements were left unchanged. Figure 4 illustrates the composition of the dimensions and groups the items into the identified concepts that are measured in each dimension.

For example, the management of the information security dimension involves four main concepts that are measured, namely accepting ownership, accepting change,

Table 6: Comparing the old and revised information security culture dimensions

Old information security culture questionnaire dimensions (factors)	Number of statements per dimension (factors)	New information security culture dimensions (factors) of ISCA	Number of statements per dimension (factors)
Information security policies	2	Management of information security	12
Information security management	2	Performance management	4
Information security programme	7	Performance accountability	3
Information security leadership	8	Communication	3
Information asset management	8	Governance	7
User management	8	Capability development	14
Change management	4		
Trust	3		
Total number of items	**42**	**Total number of items**	**43**

necessity of resources and understanding threats. The items (statements) in the information security culture questionnaire will determine users' perceptions with regard to each of the four concepts.

Table 7 outlines the statements of the revised governance dimension (previously the information assets management dimension) in order to illustrate how the statements were regrouped on the basis of the factor analysis.

CONCLUSION AND RECOMMENDATIONS

The paper addressed its purpose by validating an information security culture questionnaire. This was enabled by conducting an information security culture assessment in a financial organisation and using the data to perform a factor and reliability analysis. As output, a revised information security culture questionnaire is proposed that yields reliable results should it be used to assess information security in other organisations or as a follow-up assessment in the financial institution to benchmark the results.

In the light of the research results, it is evident that there are revised or possible additional dimensions that could be constructed for the information security culture questionnaire. Based on the assessment that was conducted, as well as other organi-

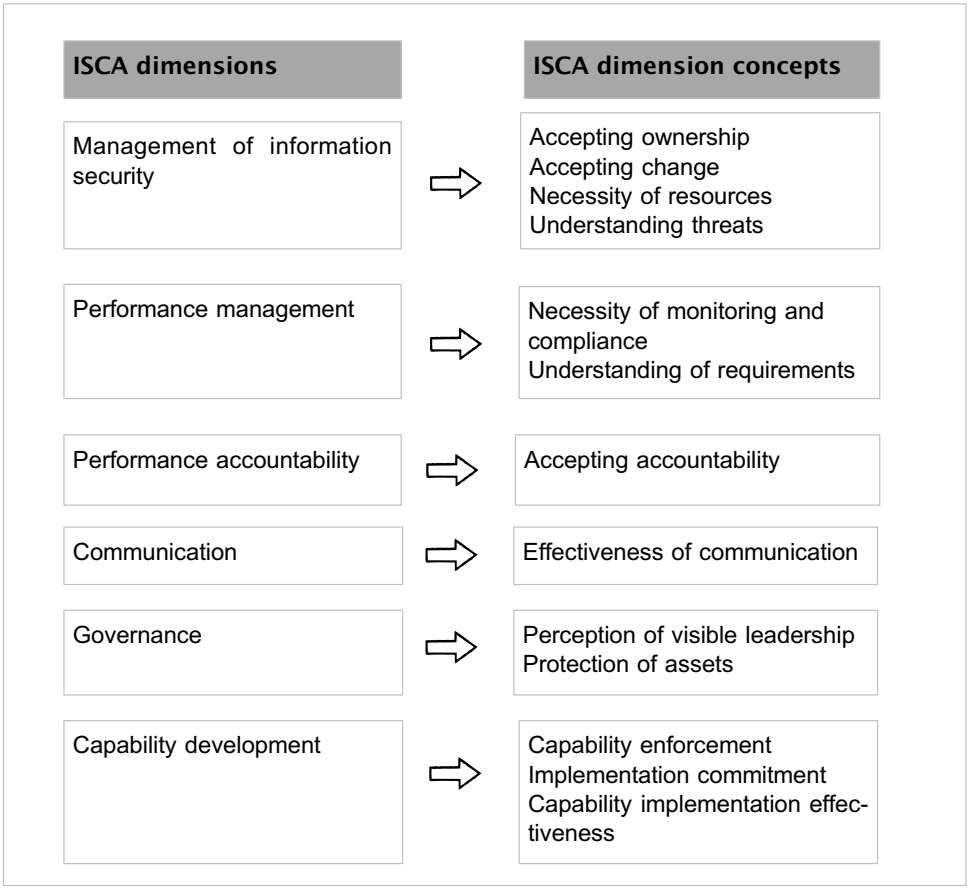


Figure 4: ISCA dimensions and concepts

Table 7: Governance dimension statements

Governance concepts	**Governance dimension statements (items)**
Perception of visible leadership	1 Management in my department **adheres** to the information security policy.
	2 Department managers and supervisors perceive information security as **important**.
	3 Executive and senior management perceive information as **important**.
	4 Information security is perceived as **important in** my business area.
	5 The staff in our department perceive information security (e.g. sharing confidential information) as **important**.
Protection of assets	6 My business area **protects** its information assets adequately.
	7 Threats to security of information assets are **adequately controlled** in my department.

sations where the information security culture assessment was conducted, it was determined that certain aspects of the information security culture questionnaire could be further enhanced to meet the needs of the industry. The following should be considered when further enhancing ISCA:

- The dimension on user knowledge and awareness could be enhanced to enable more in-depth correlations to the culture statements.
- Attention should be focused on ethical considerations and the perception of users with regard to sensitive information.
- More attention should be focused on communication in terms of what the preferred channels are and how effective employees perceive them to be.
- The performance measurement, performance accountability and communication dimensions of ISCA could be expanded to include at least three to five statements per dimension (Church & Waclawski 1998).
- The completeness of the regrouped statements in the new dimensions should be investigated. For example, the governance dimension should be assessed to identify all concepts of governance that pertain to an information security culture in order to ensure the completeness of the statements in each ISCA dimension.

REFERENCES

Abu-Musa, A.A. 2003. 'The perceived threats to the security of computerized accounting information systems', *Journal of American Academy of Business,* 3(1/2): 9–20.

Baggett, W.O. 2003. 'Creating a culture of security', *Internal Auditor*, 60(3): 37–41.

Berry, M.L. & Houston, J.P. 1993. *Psychology at Work*. Winsconsin: Brown and Benchmark.

Bresz, F.P. 2004. 'People – Often the weakest link in security, but one of the best places to start', *Journal of Health Care Compliance*, 6(4): 57–60.

Brewton, P. & Millward, L. 2001. *Organizational Research Methods*. London: Sage.

Church, A.H. & Waclawski, J. 1998. *Organizational Surveys – a Seven Step Approach*. San Francisco, CA: Jossey-Bass.

CITEC. 2005. 'Building a strong security culture'. [Online] Available at: www.citec.com.au/news/featureNews/2005/April/security_culture.shtml. Accessed: January 2006.

COBIT (Control Objectives for Information and related Technology). 2004. *COBIT Security Baseline – An Information Security Survival Kit*. USA: IT Governance Institute.

Dervin, L., Kruger, H. & Steyn, T. 2006. 'Value-focused assessment of information communication and technology security awareness in an academic enviornment', *Security and Privacy in Dynamic Environments*, pp 448–453. IFIP International Federation for Information Processing, 201.

Dillon, W.R., Madden, T.J. & Firtle, N.H. 1993. *Essentials of Marketing Research*. Boston: Irwin.

Furnham, A. & Gunter, B. 1993. *Corporate Assessment: Auditing a Company's Personality*. London: Routledge.

Gaunt, N. 2000. 'Practical approaches to creating a security culture', *International Journal of Medical Informatics*, 60(2): 151–157.

Hair, J.F., Anderson, R.E., Tatham, R.L. & Black, W.C. 1995. *Multivariate Data Analysis with Readings*, 4th edition. Englewood Cliffs, NJ: Prentice Hall.

Hintze, J.L. 1997. *Number Cruncher Statistical Systems,* version 5.03 5/90. Kaysville, UT: NCSS.

Howell, D.C. 1995. *Fundamental Statistics for the Behavioral Sciences,* 3rd edition. International Standards Organisation. [Online] Available at: www.iso.ch. Accessed: January 2005.

ISF (Information Security Forum). 2000. *Information Security Culture – A Preliminary Investigation*. United Kingdom: ISF.

ISO. 2005. Information technology. Security techniques. Code of practice for information security management. ISO/IEC 17799 (BS 7799–1: 2005).

Kraut, A.I. 1996. *Organizational Surveys*. San Francisco, CA: Jossey-Bass.

Krejcie, R.V. & Daryle, M.W. 1970. 'Determining sample size for research activities', *Educational and Psychological Measurement*, 30.

Martins, A. 2002. 'Information security culture', MCom dissertation, Rand Afrikaans University, Johannesburg.

Martins, E.C. 2000. 'Die invloed van organisasiekultuur op kreatiwiteit en innovasie in 'n universiteitbiblioteek', MCom dissertation, University of South Africa, Pretoria.

Martins, A. & Eloff, J.H.P. 2002. 'Information security culture', *Security in the Information Society,* pp. 203–214. IFIP/SEC2002. Boston, MA: Kluwer Academic Publishers.

Martins, N. & Von der Ohe, H. 2003. 'Organisational climate measurement – new and emerging dimensions during a period of transformation', *South African Journal of Labour Relations,* (27)3 & 4: 41–59.

PWC (PricewaterhouseCoopers). 2004. Information Security Breaches Survey. [Online] Available at: www.dti.gov.uk/industry_files/pdf/isbs_2004v3.pdf. Accessed: January 2005.

Robbins, S. 2001. *Organizational Behaviour,* 9th edition. New Jersey: Prentice Hall.

Robbins, S., Odendaal, A. & Roodt, G. 2003. *Organisational Behaviour – Global and Southern African Perspectives*. Cape Town: Pearson Education.

Ruighaver, A.B. & Maynard, S.B. 2006. 'Organisational security culture: More than just an end user phenomenon', *Security and Privacy in Dynamic Environments*, pp 425–430, IFIP International Federation for Information Processing, 201.

Schein, E.H. 1985. *Organizational Culture and Leadership*. San Francisco, CA: Jossey-Bass.

Schlienger, T. & Teufel, S. 2002. 'Information security culture', *Security in the Information Society*, pp 191–201. IFIP/SEC2002. Boston, MA: Kluwer Academic.

Schlienger, T. & Teufel, S. 2003. 'Analysing information security culture: Increased trust by an appropriate information security culture', Paper presented at International Workshop on Trust and Privacy in Digital Business Trust in conjunction with 14th International Conference on Database and Expert Systems Applications, Prague, Czech Republic.

Schlienger, T. & Teufel, S. 2005. 'Tool supported management of information security culture', Paper presented at 20th IFIP International Information Security Conference, Makuhari-Messe, Chiba, Japan.

Stewart, J.N. 2006. 'CSO to CSO: Establishing the security culture begins at the top'. [Online] Availabe at: cisco.com/web/about/security/intelligence/05_07_securityculture.html. Accessed: January 2006.

Survey Tracker. 2005. [Online] Available at: www.surveytracker.com. Accesed: January 2005.

Tessem, M.H. & Skaraas, K.R. 2005. 'Creating a security culture'. [Online] Availabe at: www.telenor.com/telektronikk/volumes/pdf/1.2005/Page_015–022.pdf. Accessed: January 2006.

OECD (Organisation for Economic Cooperation and Development). 2005. 'The promotion of a culture of security for information systems and networks in OECD countries (OECD)', DSTI/ICCP/REG(2005)1/FINAL.2005. [Online] Available at: www.oecd.org/document/42/0,2340,en_2649_34255_15582250_1_1_1_1,00.html. Accessed: August 2006.

Thomson, I. 2004. 'IT security culture must start from the top Global survey warns senior execs against "delegating" security awareness'. [Online] Availalbe at: www.vnunet.com/vnunet/news/2125904/securityculturestarttop. Accessed: January 2006.

Von Solms, B. 2000. 'Information security – the third wave?' *Computers and Security*, 19(7): 615–620.

Von Solms, B. 2006. 'Information security – the fourth wave', *Computers and Security,* 25 (2006): 165–168.

Zakaria, O. 2006. 'Internalisation of information security culture amongst employees through basis security knowledge', *Security and Privacy in Dynamic Environments*, pp 437–441. IFIP International Federation for Information Processing, 201.

APPENDIX E – PAPER PUBLISHED IN JOURNAL: AN INFORMATION SECURITY GOVERNANCE FRAMEWORK

Information Systems Management, 24:361–372, 20
Copyright © Taylor & Francis Group, LLC
ISSN: 1058-0530 print/1934-8703 online
DOI: 10.1080/10580530701586136

Taylor & Francis
Taylor & Francis Group

An Information Security Governance Framework

A. Da Veiga
PhD Student,
University of Pretoria,
South Africa.

J. H. P. Eloff
Head of Department and
Professor of Computer Science,
Department of Computer Science,
University of Pretoria,
South Africa.

ABSTRACT Information security culture develops in an organization due to certain actions taken by the organization. Management implements information security components, such as policies and technical security measures with which employees interact and that they include in their working procedures. Employees develop certain perceptions and exhibit behavior, such as the reporting of security incidents or sharing of passwords, which could either contribute or be a threat to the securing of information assets. To inculcate an acceptable level of information security culture, the organization must govern information security effectively by implementing all the required information security components. This article evaluates four approaches towards information security governance frameworks in order to arrive at a complete list of information security components. The information security components are used to compile a new comprehensive Information Security Governance framework. The proposed governance framework can be used by organizations to ensure they are governing information security from a holistic perspective, thereby minimising risk and cultivating an acceptable level of information security culture.

KEYWORDS information security governance framework, information security components, information security culture, information security behavior

INTRODUCTION

Information security encompasses technology, processes, and people. Technical measures such as passwords, biometrics, and firewalls alone are not sufficient in mitigating threats to information. A combination of measures is required to secure systems and protect information against harm. Processes such as user registration and de-registration and people aspects such as compliance, training and leading by example need to be considered when deploying information security. As the deployment of information security evolved, the focus has been shifting towards a people-orientated and governance-orientated approach.

The so-called first phase of information security was characterised by a very technical approach in securing the IT environment. As time went by, the "technical people" in organizations started to realize that management played a significant role in information security and that top management

Address correspondence to
A. Da Veiga,
PO Box 741, Glenvista,
Johannesburg, 20098, South Africa.
E-mail: adele.daveiga@kpmg.co.za

needed to become involved in it too (2000). This led to a second phase, where information security was incorporated into organizational structures. These two phases, namely technical protection mechanisms and management involvement have since continued in parallel. Organizations came to realize that there were other elements of information security that had been disregarded in the past. They concluded that the human element, which poses the greatest information security threat to any organization, urgently needs to be addressed (Da Veiga, Martins, & Eloff, 2007; Von Solms, 2000, 1997) and more attention be given to the information security culture within organizations (Von Solms, 2000). This third phase of information security emphasizes that information security should be incorporated into the everyday practices performed as part of an employee's job to make it a way of life and so cultivate an effective information security culture throughout the organization. An information security culture is defined as the assumption about those perceptions and attitudes that are accepted and encouraged in order to incorporate information security characteristics as the way in which things are done in an organization (Martins & Eloff, 2002).

According to the Cobit Security Baseline (2004), executives are responsible for communicating the right information security culture and control framework and for exhibiting acceptable information security behavior. This relates to the fourth phase of information security, namely the development and role of information security governance (Von Solms, 2006). Information security governance can be described as the overall manner in which information security is deployed to mitigate risks.

One of the key drivers in the fourth phase is the prevention of risks such as fraud and social engineering. The Information Security Breaches Survey conducted by PriceWaterhouseCoopers (PWC, 2004) stated that the number of technology-related security incidents such as system failures or data corruptions organization experience is very high, but that "human error rather than flawed technology is the root cause of most security breaches" (PWC, 2004). According to PriceWaterhouseCoopers, the solution would be to create a security-aware culture. Management is starting to realize that human interaction with technical controls could lead to serious fraud or social engineering. Von Solms (2006), consequently emphasises that good information security governance is essential to address these risks.

The risks faced by the organization can only be addressed when a governance framework for information security is in place and equipped with specific controls that executives may use to direct employee behavior. Such a governance framework can enable organizations to make provisions for human behavior in their information security initiatives, in order to cultivate an acceptable level of information security culture. In other words, there is a need for an information security governance framework that considers the technical and procedural controls of the past, but that also takes human behavior into account. Such a framework can be utilized to cultivate the acceptable level of information security culture in order to minimize risks posed to information assets.

The purpose of this article is to evaluate four current approaches towards information security governance frameworks in order to construct a new comprehensive Information Security Governance framework. This new Information Security Governance framework considers technical, procedural and human behavioral components to provide an all-encompassing and single point of reference for governing information security. The four approaches that are evaluated in the following section are ISO 17799 (2005), PROTECT (Eloff & Eloff, 2005), the Capability Maturity Model (McCarthy & Campbell, 2001), and the Information Security Architecture (ISA) (Tudor, 2000). The third section provides a comprehensive list of information security components based on the components of the four mentioned approaches. The information security components are used to construct the Information Security Governance framework (see Figure 1). Finally, the Information Security Governance framework is proposed and discussed in the last section.

INFORMATION SECURITY GOVERNANCE FRAMEWORKS—EXISTING APPROACHES

Information security behavior could be explained by illustrating the security we implement in our

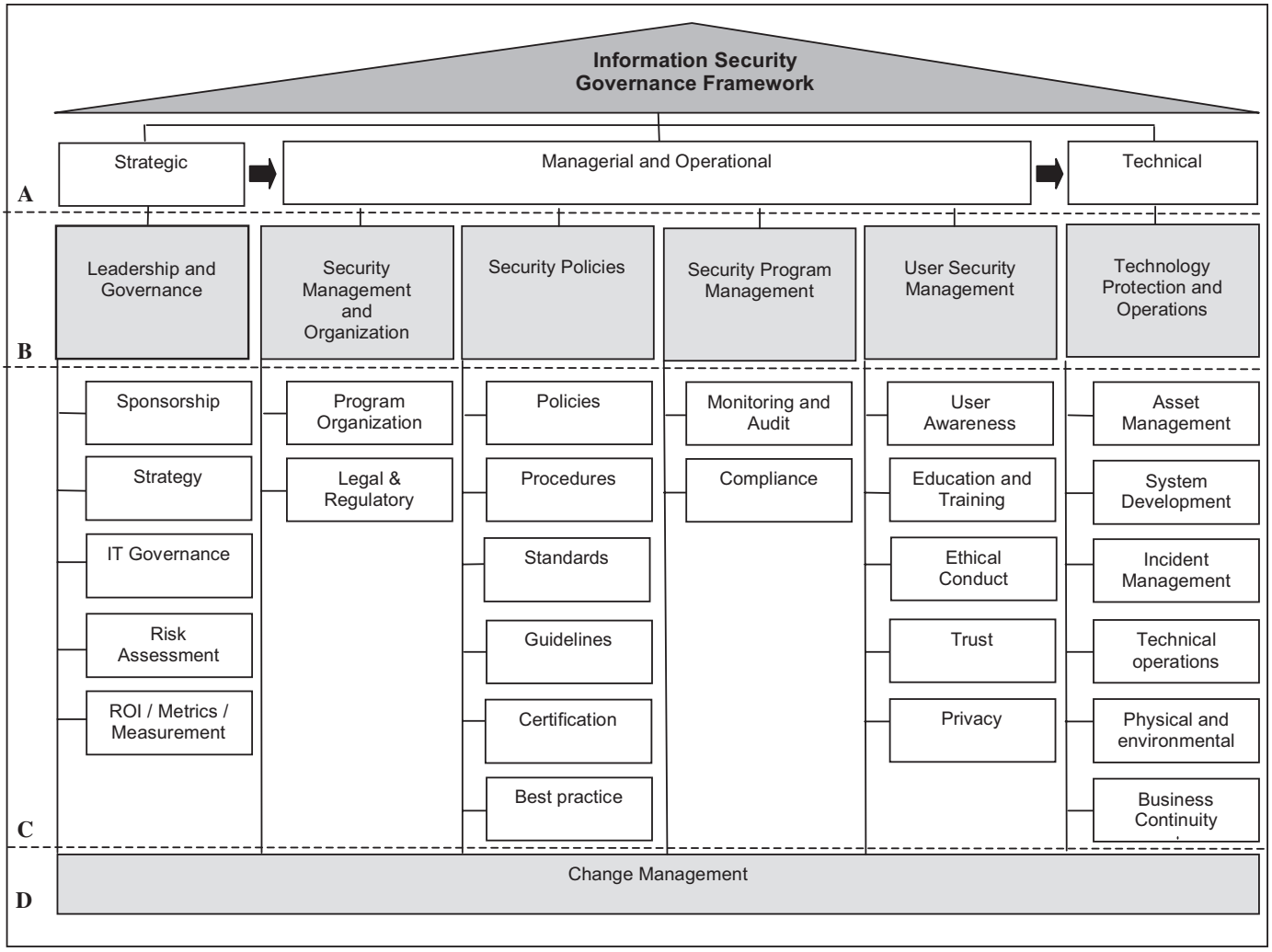


FIGURE 1 **Information Security Governance framework.**

houses. A homeowner could implement burglar proofing at each window, but upon leaving the house leave the front door unlocked. The security measures are therefore ineffective due to his behavior. In the same way, organizations implement security controls such as anti-virus programs, firewalls, and passwords. There is no sense in implementing these controls if users share passwords and connect through dialup to the Internet, bypassing the firewall.

The behavior of employees needs to be directed and monitored to ensure compliance with security requirements. As such, management needs to implement and communicate specific security controls—also referred to as components (Tudor, 2000; ISO 17799, 2005) —before they can expect employees to adhere to and exhibit an acceptable level of information security culture.

Various researchers and organizations have defined the components of information security and how an organization should go about implementing them (ISO 17799, 2005; Tudor, 2000; McCarthy & Campbell, 2001; Teufel, 2003). Information security components can be described as the principles that enable the implementation and maintenance of information security—such as an information security policy, risk assessments, technical controls, and information security awareness. These components can be encompassed in an information security governance framework where the relationship between the components is illustrated. The Information Security Governance framework provides organizations with an understanding of the requirements for a holistic plan for information security. It also combines technical, procedural, and people-orientated components for the purpose of cultivating an

appropriate level of information security minimising risks posed to information assets.

The subsequent sections provide a description of four current approaches to information security governance frameworks in order to define and construct a comprehensive new Information Security Governance framework (Figure 2).

ISO/IEC 177995 and ISO/IEC 27001

The Information Technology Security techniques—Code of Practice for Information Security Management (ISO/IEC 17799, 2005) of the Information Security Organization (ISO) take the form of guidance and recommendations and are intended to serve as a single reference point for identifying the range of controls needed for most situations where information systems are used. ISO/IEC 17799 (2005) has gradually gained recognition as an essential standard for information security (ISO/IEC, 2005). It consists of the 11 control sections detailed in Table 1.

The certification standard ISO 27001 (2005) is regarded as part two of ISO/IEC 17799 (2005) and proposes an approach of continuous improvement through a process of establishing, implementing, operating, monitoring, reviewing, maintaining and improving the organization's information security management system (ISO, 2005; IEC, 2005). The previously mentioned international standards are considered as a single encompassing approach since ISO/IEC 17799 (2005) details the components of information security and ISO/IEC 27001 (2005) outlines the approach aimed at implementing and managing them.

PROTECT

The research conducted by Eloff and Eloff (2005) introduced a comprehensive approach towards information security, namely PROTECT. This is an acronym for Policies, Risks, Objectives, Technology, Execute, Compliance, and Team. PROTECT is aimed at addressing all aspects of information security. It involves an approach that considers various and well-integrated controls in order to minimize risk and ensure effectiveness and efficiency in the

ntrol Sections of ISO/IEC 17799
(Adapted from ISO/IEC 17799, 2005)

1. **Security policy** that aims to provide management direction and support for information security, including laws and regulations.
2. **Organization of information security** that constitutes the process implemented to manage information security within the organization.
3. **Asset management** that focuses on asset inventories, information classification, and labeling.
4. **Human resources** security that considers permanent, contractor, and third-party user responsibilities to reduce the risk of theft, fraud, and misuse of facilities. This section also includes awareness, training, and education of employees.
5. **Physical and environmental** security controls that allow only authorized access to facilities and secure areas.
6. **Communications and operations management** that focus on the correct and secure operation of information-processing facilities, such as segregation of duties, change management, malicious code, and network security.
7. **Access controls** that manage user access to information and include clear desk principles, network access controls, operating system access controls, passwords, and teleworking.
8. Information **systems acquisition, development, and maintenance** that ensure the security of user-developed and off-the-shelf products.
9. Information security **incident management** that ensures that incidents are communicated in a timely manner and that corrective action is taken.
10. **Business continuity management** that focuses on business continuity plans and the testing thereof.
11. **Compliance** in terms of statutory, regulatory or contractual, laws, audit and organizational policy requirements, or obligations.

organization. The seven control components of PROTECT are aimed at implementing and managing an effective information security program from a technology perspective as well as a people perspective and are summarised in Table 2.

Capability Maturity Model

The Capability Maturity Model (McCarthy & Campbell, 2001) approach provides a set of security controls used to protect information assets against unauthorised access, modification or destruction. The model is based on a holistic view of information security and encompasses seven main control levels as portrayed in Table 3.

TABLE 2 Control Components of PROTECT (Adapted from Eloff & Eloff, 2005)

1 The **policy** component includes information security policies, procedures, and standards, as well as guidelines for maintaining these.
2 **Risk** methodologies such as CRAMM and Octave, as well as automated tools to identify system vulnerabilities are covered in the risk component.
3 **Objective** refers to the main objective of PROTECT, namely to minimize risk exposure by maximizing security through the implementation and monitoring of a comprehensive set of controls.
4 **Technology** refers to hardware, software, and systems product components of the IT infrastructure and, where possible, the use of certified products.
5 Information security controls need to be established, maintained, and managed. **Execute,** therefore, refers to a proper information security management system environment.
6 The **compliance** component covers both internal compliance with the organization's policies and external compliance with information security expectations set by outside parties to the organization. Compliance also includes international codes of practice, legal requirements, and international standards.
7 **Team** refers to the human component, namely all the employees of the organization, where each has a responsibility towards securing information. The objective is to create a security-aware workforce that will contribute to an improved information security culture.

ntrols Levels of the Capability Maturity Model (Adapted from McCarthy & Campbell, 2001)

1 **Security leadership:** Security sponsorship/posture, security strategy, and return on investment/metrics.
2 **Security program**: Security program structure, security program resources, and skill sets.
3 **Security Policies**: Security policies, standards, and procedures.
4 **Security Management**: Security operations, security monitoring, and privacy.
5 **User Management**: User management and user awareness.
6 **Information Asset Security:** Application security, database/meta security, host security, internal and external network security, anti-virus, and system development.
7 **Technology Protection & Continuity**: Physical and environmental controls and continuity-planning controls.

The first level, security leadership, stresses the importance of an executive level security representative and an information security strategy. This should be the starting point for deploying both a long-term and short-term information security strategy within an organization. Next, a security program with defined roles and responsibilities for information security tasks should be developed and implemented. The roles of inter alia information security officer, network specialist, anti-virus specialist, database specialist, and Helpdesk personnel need to be defined. On the third level, security policies, standards, and guidelines need to be compiled to direct the implementation of information security. These policies, standards, and guidelines should cover the technical, procedural, and human aspects of information security. Security management will then form part of day-to-day operations, which include the monitoring of users and the technology deployed as directed by the previous layers. The organization subsequently needs to ensure that users are aware of policies and that user profiles are managed. Finally, the approach addresses information asset security that encompasses the technology aspects of information security, such as configuring a secure firewall, network and database. Technology protection comprises the last layer and focuses not only on the IT environment and its continuity, but also includes business continuity and disaster recovery.

The objective of the Capability Maturity Model approach is to start from the top on a strategic level and work down to the technology levels, guided by the direction provided by the strategic levels. In implementing information security, the model is used to assess the current information security capability and risks and to architect the appropriate solution to mitigate risks. The solution as well as monitoring capabilities are then implemented and integrated with current processes.

Information Security Architecture (ISA)

Tudor (2000) proposes a comprehensive and flexible Information Security Architecture (ISA) approach to protect an organization's assets against threats. This approach highlights five key principles, listed in Table 4, that are used to understand the risk environment in which organizations operate in order to evaluate and implement controls to mitigate such risks. There is also a focus on country regulations to ensure that each organization's confidential

TABLE 4 Principles of the Information Security (Adapted from Tudor, 2000)

1. **Security organization and infrastructure:** Roles and responsibilities are defined and executive sponsorship is established.
2. **Security policies, standards, and procedures**: Policies, standards and procedures are developed.
3. **Security program:** A security program is compiled taking risk management into account.
4. **Security culture awareness and training:** Users are trained and awareness is raised through various activities. Trust among users, management, and third parties are established.
5. **Monitoring compliance:** Internal and external monitoring of information security is conducted.

information is protected accordingly. The principles encompass aspects of process, as well as technology to address organizations' security needs.

The first principle relates to security organization and infrastructure with defined roles and responsibilities, as well as to executive sponsorship. The second principle requires that security policies, standards and procedures supported by management be developed and implemented. Security control requirements stated in the security policies cannot be deployed in isolation, but must be considered in terms of the risks the organization faces. Therefore, as a third principle, risk assessments must be performed across platforms, databases, applications, and networks, and a process should be instituted to provide an adequate budget for resources to address risks and implement controls. In order for the controls to operate effectively, users need to be made aware of their responsibility and encouraged to attend training programs. This fourth principle aims to establish an environment of trust among users, management and third parties to enable transactions and protect privacy. The fifth and last principle focuses on compliance testing and audits by internal and external auditors to monitor the effectiveness of the security program. The number of security incidents and Internet sites visited, as well as the levels of network and email usage constitutes aspects that must be monitored to allow a proactive approach towards addressing threats to information. In Tudor's latest research, aspects such as business continuity and disaster recovery are included as part of the approach aimed at preserving organizational information and assets (Holborn, 2005).

COMPREHENSIVE LIST OF INFORMATION SECURITY COMPONENTS

A comprehensive list of components was compiled from the relevant sections of ISO 17799, components of PROTECT, levels of the Capability Maturity Model and principles of the ISA approach. These components were selected from each approach where a component was depicted as a key principle (e.g., "risk focus"), or as an information security control (e.g., "business continuity"). Where components overlapped between approaches such as "policies," a combined component category was defined.

A comprehensive list of components is presented in Table 5. The objective of Table 5 is to consolidate the components of the various approaches as discussed in the previous paragraph. It also shows the % representation of each approach's components. This comprehensive list of components forms the basis of the Information Security Governance framework, as discussed in the next section. Each component addressed by a specific approach is indicated on Table 5 by an inclusion tick ("•"). The sum of the ticks is divided by the total number of components to give the percentage of representation for each approach. This is depicted at the bottom of the table (ISO17799—68%, Eloff and Eloff—63%, McCarthy and Campbell—77%, and Tudor—59%).

Based on the assessment of the approaches, the components of ISO/IEC 17799 (2005) and the Capability Maturity Model of McCarthy and Campbell are the most comprehensive in addressing the breadth of information security components and therefore the percentage representation is higher compared to the approach of Eloff and Eloff and Tudor. Corporate governance, ethical conduct, and trust are not included in either of these two approaches, although all three components are considered by various researchers (Donaldson, 2005; Flowerday & Von Solms, 2006; Trompeter & Eloff, 2001) when governing information security in an organization.

The approach put forward by Eloff and Eloff (2005) suggests a holistic set of controls to consider and focuses mainly on providing a standardised approach for the management of an information security program. It is the only approach that mentions ethical values. Employees need to integrate

TABLE 5 Information Security Governance App

	Information security components	ISO 17799 (2005)	Eloff & Eloff	McCarthy & Campbell	Tudor
1	Corporate governance	X	X	X	X
2	Information security strategy	X	X	•	X
3	Leadership in terms of guidance and executive level representation	•	•	•	•
4	Security organization (internal organization such as management commitment, responsibilities, and coordination; external parties)	•	•	•	•
5	Security policies, standards, and guidelines	•	•	•	•
6	Measurement / Metric / Return on investment	X	•	•	X
7	Compliance and monitoring (legal, regulatory, and auditing)	•	•	•	•
8	User management (user, joiner, and leaver process)	•	X	•	X
9	User awareness, training, and education	•	•	•	•
10	Ethical values and conduct	X	•	X	X
11	Privacy	X	X	•	X
12	Trust	X	X	X	•
13	Certification against a standard	•	•	X	X
14	Best practice and baseline consideration	•	•	•	•
15	Asset management (responsibility and classification)	•	•	X	•
16	Physical and environmental controls (secure areas and equipment)	•	•	•	•
17	Technical operations (e.g., anti-virus, capacity, change management, and system development)	•	•	•	•
18	System acquisition, development, and maintenance	•	•	•	X
19	Incident management	•	X	•	X
20	Business continuity planning (BCP)	•	X	•	•
21	Disaster recovery planning (DRP)	X	X	•	•
22	Risk assessment process	•	•	•	•
Number of components derived from each approach		**15**	**14**	**17**	**13**
Percentage		**68%**	**63%**	**77%**	**59%**

ethical conduct or behavior relating to information security into their everyday life in the organization (Trompeter & Eloff, 2001). According to Baggett (2003), it is the responsibility of management and the board to develop and distribute corporate codes of conduct that should cover both commercial and social responsibilities. Ethical conduct, for example, not copying organizational software at home or using the Internet for private purposes during working hours, needs to be enforced as the accepted way of conduct in the work environment in order for the desired information security culture to emerge. Although the Eloff approach (Eloff & Eloff, 2005) is very comprehensive, it does not mention aspects such as business continuity or incident management. These could, however, be covered under the policy and procedures component.

Only Tudor (2000) mentions trust in his approach. According to Von Solms (2000), trust is arguably the most important issue in establishing information security in an IT environment. If management trusts its employees and the employees trust management, it is easier to implement new procedures and guide employees through changes of behaviour pertaining to information security. Corporate governance, ethical considerations and trust would all need to be incorporated into the approach adopted by an organization to provide a comprehensive set of information security components that can deal with its risks such as attempts at social engineering, fraud and staff misuse of information systems.

A NEW APPROACH TO AN INFORMATION SECURITY GOVERNANCE FRAMEWORK

In consolidating the four approaches towards information security governance discussed above,

one assembles a comprehensive set of c onsists of a comprehensive list of information security components categorised under each of the six main categories (level B). All six of the main categories are influenced by change depicted at the bottom of the figure (level D).

to consider for information security governance. The proposed Information Security Governance framework (see Figure 2) can be used as a starting point by an organization to govern information security by developing guidelines and implementing controls to address risks identified by the organizations, such as misuse of web browsing, data corruption, or identify theft. This new framework can be utilized to govern employee behavior in all required facets of information security and cultivating an acceptable level of information security culture.

Ultimately, this governance framework provides management the means to implement an effective and comprehensive information security governance program that addresses technical, procedural, and human components. It integrates the components of the four discussed approaches, as well as components not considered, such as trust. Hence, the framework provides a single point of reference for the governance of information security to inculcate an acceptable level of information security culture. As each organization's environment is different and subject to different national and international legislation and regulations, additional components might be required, while others may not be relevant.

The information security governance framework, Figure 2, is partitioned into four levels, namely A, B, C, and D. Level A consists of strategic, managerial/implementation and technical protection components. The strategic components, shown on the left side of the figure, provide direction to the managerial and operational implementation components, depicted in the middle section of the figure. The technical protection components are shown on the right side of Figure 2.

Level B consists out of six main categories which are grouped according to the three Level A categories. The six main categories are:

- Strategic:
  - Leadership and governance.
- Managerial and Operational:
  - Security management and organization;
  - Security policies;
  - Security program management; and
  - User security management.
- Technical:
  - Technology protection and operations.

Implementing the information security components institutes change in the organization's processes and will influence the way people conduct their work. An important consideration is that organizations do not change, but people do, and therefore people change organizations (Verton, 2000). Information security changes in the organization need to be accepted and managed in such a way that employees are able to successfully incorporate such changes into their work. The component indicated as "Change" (Figure 2), needs to be considered when implementing any of the information security components. The six main categories (level B) of information security components and the composition thereof are discussed below.

Leadership and Governance

This category comprises executive level sponsorship for information security, as well as commitment from the board and management to protect information assets. This is due to the fact that information security governance is accepted as an integral part of good IT and Corporate Governance (Von Solms, 2005). Corporate governance refers to organization controls such as reporting structure, authority, ownership, oversight, and policy enforcement (Knapp, Marshall, Rainer, & Morrow, 2004). Corporate governance relates to the responsibility of the board to effectively direct and control an organization through sound leadership efforts (King Report, 2001; Donaldson, 2005). This is associated with IT governance, which is concerned about the policies and procedures that define how an organization will direct and control the use of its technology and protect its information (Posthumus & Von Solms, 2005).

Based on a study conducted by Gartner (Security, 2005), some of the top 10 business and technology priorities of Chief Information Officers (CIOs) in 2005 were to implement security enhancement tools, and to address security breaches and disruptions, as well as privacy issues. These actions would illustrate that

management is realising that information can add great value to the organization – which is the starting point for illustrating information security leadership.

The leadership and governance category also involves the compilation of an information security strategy that addresses information threats by conducting risk assessments aimed at identifying mitigation strategies and required controls. The information security strategy should be linked to the organizational and IT strategy to ensure that the organization's objectives are met both in the short and in the long term.

Finally, the category includes the concepts of metrics and measurement to measure how effective the organization is in addressing threats to information security. Many organizations are turning to metrics to evaluate the overall effectiveness of their information security programs (Witty & Hallawell, 2003) and whether it contributes in achieving the organization's strategy. The number of security incidents or even empirical results of awareness surveys can be used as metrics. Metrics will assist organizations in converting today's security threats into tomorrow's business opportunities (Ponemon, 2005).

Security Management and Organization

Program organization and legal and regulatory considerations are covered in this category. The objective of the category is to manage information security within the organization (ISO 17799, 2005). Program organization refers to the information security organizational design, composition and reporting structures (e.g., centralized or decentralized management of security). It also incorporates the roles and responsibilities, skills and experience, and resource levels committed to the enterprise security architecture (McCarthy & Campbell, 2001).

Different pieces of national and international legislation need to be considered for information security—for example, the Health Insurance Portability and Accountability Act (HIPAA) (Bresz, 2004); the Sarbanes-Oxley Act (Donaldson, 2005); the King Report II (2001); the Electronic Communications and Transactions Act (ECT) (2002); and the Promotion of Access to Information Act (PROATIA) (2000).

Security Policies

Security policies, procedures, standards, and guidelines are key to the implementation of information security in order to provide management with direction and support (ISO 17799, 2005) and they should clearly state what is expected of employees and guidelines for their behavior (Richards, 2002). ISO 17799 (2005) defines a policy as an "overall intention and direction as formally expressed by management." The security policies should consider the categories mentioned earlier (e.g., legal considerations) and must be implemented in the organization through effective processes and compliance monitoring. Examples of information security policies are an access control policy, e-mail, and Internet policy and a physical and environmental policy. A procedure such as a user registration and deregistration procedure explains or spells out statements of the security policy and is the steps that need to be taken to accomplish the policy (Von Solms & Von Solms, 2004). Procedures are underpinned by standards such as a password standard and guidelines for example how to configure a firewall to meet the requirements of the security policy.

Security Program Management

Monitoring and compliance as well as auditing are included in this category, which involves management of the security program. It is essential to measure and enforce compliance (Von Solms, 2005), and both technology and employee behavior (Vroom & Von Solms, 2004) should be monitored to ensure compliance with information security policies and to respond effectively and timely to incidents that are detected. Monitoring of employee behavior could include monitoring the installation of unauthorized software, the use of strong passwords or Internet sites visited. Technology monitoring could relate to capacity and network traffic monitoring. Information security auditing is necessary to ensure that the policies, processes, procedures and controls are in line with the objectives, goals and vision of the organization (Vroom & Von Solms, 2004).

User Security Management

This category addresses user awareness; education and training; ethical conduct; trust and privacy. ISO/IEC 17799 (2005) states that the organization must have plans and programs in place to implement, maintain, and effectively promote information security awareness and education throughout the organization.

According to the Guidelines for the Security of Information Systems and Networks of the Organization for Economic Cooperation and Development (OECD) (Baggett, 2003), one of the principles in creating a security culture is ethical conduct—where both management and the board develop and communicate corporate codes of conduct. Hellriegel, Slocum, and Woodman (1998) define ethics as the values and rules that distinguish right from wrong. It is management's responsibility to establish ethical standards of conduct that are in essence rules to be followed by employees and to be enforced by the organization (Cardinali, 1995). As part of the information security governance framework, ethical conduct must be addressed by the organization to minimize the risk of for instance invasion of privacy, selling of customer information and unauthorised altering of data. These rules should be communicated to employees as part of the security awareness programme.

N. Martins (2002) defines trust as "the process in which a trustor relies on a trustee (a person or group of people) to act according to specific expectations that are important to the trustor without taking advantage of the trustor's vulnerability." When implementing the Information Security Governance framework components, management must be able to trust employees to adhere to information security policies, while employees must be able to trust management to demonstrate commitment to information security (trust is seen as the primary attribute of leadership) (Robbins, Odendaal, & Roodt, 2001). A trusting relationship should also be established between trading partners and clients who could contribute to the organization's reputation. One possible way of establishing such a relationship could be for the organization to illustrate that information and assets are secured and that employees comply with requirements.

; an essential issue of trust when it comes to good relationships with customers, suppliers and other business partners (Tretic, 2001). If there is no privacy in business, there will be no trust (Ross, 2000). When implementing information security privacy, both employees and customers must be considered and controls must be implemented to protect their identity.

Technology Protection and Operations

The technology protection and operations category relates to the traditional focus of information security. It involves the technical and physical mechanisms implemented to secure an IT environment (Von Solms, 1997; Von Solms, 2000). When implementing the security governance framework, the technology controls applicable to the organization's environment and identified risks must be implemented. These include asset management, system development requirements, incident management, technical operations such as network security, and physical, environment, and business continuity controls. It is essential that the technology environment be monitored on a constant basis and that the risks of technology changes in the market be addressed—e.g., the use of personal digital assistants and teleworking technology.

CONCLUSION

The first step in developing an information security culture and empowering the workforce to be aware of their responsibilities towards protecting information assets would be to implement a comprehensive Information Security Governance framework—as is proposed in this article. It is evident that one approach alone is not sufficient in governing information security, but that an integrated approach should be adopted to ensure that all components pertaining to information security is considered. The new Information Security Governance framework can be deployed by organizations as a comprehensive and single point of reference towards governing information security. It considers a broad spectrum of components to assist in addressing risks to infor-

mation assets on a technology, processes level. Management and executives can use the Information Security Governance framework as a reference for governing information security in all facets of the organization's information asset environment. The implementation of the applicable components of the Information Security Governance framework in an organization should have a positive impact on the behavior of employees and on how they protect the organization's assets, thereby minimising risks to information assets and cultivating an acceptable information security culture. The governance framework can be used in future research as a reference to develop an information security culture assessment tool to measure whether the level of information security culture is on an acceptable level, and to employ action plans for areas of development.

References

Baggett, W. O. (2003). Creating a culture of security. *The Internal Auditor*, *60* (3), 37–41.

Bresz, F.P. (2004). People—Often the weakest link in security, but one of the best places to start. *Journal of Health Care Compliance*, *6* (4), 57–60.

Cardinali, R. (1995). Reinforcing our moral vision: Examining the relationship between unethical behaviour and computer crime. *Work Study. 44* (8), 11–18.

COBIT security baseline—An information security survival kit. (2004). Rolling Meadows, USA: IT Governance Institute.

Da Veiga, A., Martins, N., & Eloff J. H. P. (2007). Information security culture—validation of an assessment instrument. *Southern African Business Review, 11* (1): 147–166.

Donaldson, W. H. (2005). U.S. capital markets in the post-Sarbanes-Oxley world: Why our markets should matter to foreign issuers. *U.S. Securities and Exchange Commission*. London School of Economics and Political Science.

Electronic Communications and Transactions Act. (2002). Retrieved 12 January 2006 from site: http://www.acts.co.za/ect_act/

Eloff, J. H. P. & Eloff, M. (2005). Integrated Information Security Architecture, *Computer Fraud and Security*, *2005* (11), 10–16.

Flowerday, S., & Von Solms, R. (2006). Trust an element of information security. In *Security and Privacy in Dynamic Environments*. IFIP/SEC2005; Boston: Kluwer Academic Publishers, 87–97.

Hellriegel, D., Slocum, J. W. (Jr), & Woodman, R. W. (1998). *Organizational Behavior*. (8th ed.). Cincinnati, OH: South-Western College Publishing. Holborn Books. Information Security architecture: An integrated approach to security in the organization (2005). Retrieved 18 April 2005 from: http://www.holbornbooks.co.uk/details.aspx?sn=1244811

ISO/IEC 17799 (BS 7799-1) (2005). Information technology. Security techniques. Code of practice for information security management, Britain.

ISO/IEC 27001 (BS 7799-2) (2005). Information technology. Security techniques. Information security management systems—requirements, Britain.

King Report. (2001). The King Report of corporate governance for South Africa. Retrieved 12 January 2006: http://www.iodsa.co.za/downloads/King%20II%20Report%20CDRom%20Brochure.pdf

arshall, T. E., Rainer, R. K., & Morrow, D. W. (2004). Top ranked information security issues: *The 2004 International Information Systems Security Certification Consortium (SIC) survey results*. Auburn, Alabama: College of Business Auburn University.

McCarthy, M. P. & Campbell, S. (2001). *Security Transformation*. McGraw-Hill: New York.

Martins, A. (2002). *Information Security Culture*. Master's dissertation, Rand Afrikaans University, Johannesburg, South Africa.

Martins, A. & Eloff, J. H. P. (2002). Information Security Culture. In *Security in the information society. IFIP/SEC2002*. (pp. 203–214). Boston: Kluwer Academic Publishers.

Martins, N. (2002). A model for managing trust. *International Journal of Manpower. 23* (8), 754–769.

The Concise Oxford Dictionary. (1983). Sykes, J.B. (Ed.) Oxford: Clarendon Press.

Posthumus, S. & Von Solms, R. (2005). IT Governance. *Computer Fraud and Security. 2005* (6), 11–17.

PriceWaterhouseCoopers. Information Security Breaches Survey. (2004). Retrieved 12 March 2005 from http://www.dti.gov.uk/industry_files/pdf/isbs_2004v3.pdf

Promotion of Access to Information Act. (2000). Retrieved 12 January 2006 from http://www.acts.co.za/prom_of_access_to_info/index.htm

Richards, N. (2002). The critical importance of information security to financial institutions. *Business Credit*, *104* (9), 35–36.

Robbins, S. (2001). *Organizational Behaviour*. (9th ed.). New Jersey: Prentice Hall.

Ross, B. (2000). New directives beef up trust in e-commerce. *Computer Weekly News*.

Security. 2005. Security, innovation head CIO's 2005 agenda. *Computer Fraud and Security*, *2005* (1), 1–2.

Teufel, S. (2003). Information Security Management—State of the art and future trends. In *Proceedings of the Annual International Information Security South Africa (ISSA) conference*. Johannesburg, SA, UNISA Press.

Tretic, B. (2001 January). Can you keep a secret? *Intelligent Enterprise*. *4* (1).

Trompeter, C. M. & Eloff, J. H. P. (2001). A framework for the implementation of Socio-ethical controls in Information Security. *Computers and Security*, *20* (5), 384–391.

Tudor, J. K. (2000). *Information Security Architecture—An integrated approach to security in an organization*. Boca Raton, FL: Auerbach.

Verton, D. (2000). Companies aim to build security awareness. *Computerworld*, *34* (48), 24.

Von Solms, R. (1997). Driving safely on the information superhighway. *Information Management & Computer Security*, *5* (1), 20–22.

Von Solms, B. (2000). Information security—The third wave? *Computers and Security*, 19(7). November, 615-620.

Von Solms, S. H. (2005). Information Security Governance—Compliance management vs. operational Management. *Computers and Security*, *24* (6), 443–447.

Von Solms, S. H. (2006). Information Security—The fourth wave. *Computers and Security. 25* (2006), 165–168.

Vroom, C., & Von Solms, R. (2004). Towards information security behavioural compliance. *Computers and Security*, *23* (33), 191–198.

Witty, R. J. & Hallawell, A. (2003). Client issues for security policies and architecture. *Gartner*. ID number: K-20-7780.

BIOGRAPHIES

Adele da Veiga is currently completing her PhD (IT) focusing on information security culture at the University of Pretoria, South Africa. She is a management consultant focusing on information security, risk management, and auditing.

JHP Eloff received a PhD (Computer Sc[illegible]f Pretoria. He has published extensively the Rand Afrikaans University, South Africa. He gained practical experience by working as management consultant specializing in the field of information security. He is the Head of Department and full professor in Computer Science at the Department of Computer Science, in a wide spectrum of accredited international subject journals. He is evaluated as a B2 researcher from The National Research Foundation (NRF), South Africa. He is a member of the Council for Natural Scientists of South Africa.