TOWARDS A FRAMEWORK TO ENSURE ALIGNMENT AMONG INFORMATION SECURITY PROFESSIONALS, ICT SECURITY AUDITORS AND REGULATORY OFFICIALS IN IMPLEMENTING INFORMATION SECURITY IN SOUTH AFRICA

MANDLA BASANI

TOWARDS A FRAMEWORK TO ENSURE ALIGNMENT AMONG INFORMATION SECURITY PROFESSIONALS, ICT SECURITY AUDITORS AND REGULATORY OFFICIALS IN IMPLEMENTING INFORMATION SECURITY IN SOUTH AFRICA

by

MANDLA BASANI

Submitted in fulfilment of the requirements

for the degree of

MASTER OF SCIENCE

in the subject

COMPUTER SCIENCE

at the

UNIVERSITY OF SOUTH AFRICA

SUPERVISOR: MARIANNE LOOCK

FEBRUARY 2012

Acknowledgement

I would like to express my appreciation to the following people:

- My fiancée, **Penelope**, for her support and for looking after our children while I worked for long hours on this dissertation.

- My children, **Nomalungelo** and **Malwande**, for being a glimmer of hope when completing the dissertation seemed like a high mountain to climb.

- **Marianne Loock**, for being an outstanding supervisor, a leader and a role model who kept providing guidance and insightful feedback on my work. It was an honour and a privilege to have had a supervisor of your calibre.

- **Prof Elmarie Kritzinger**, for her patience, work ethic and positive attitude, which she instilled in me through our interactions and her constructive feedback.

Abstract

Information security in the form of IT governance is part of corporate governance. Corporate governance requires that structures and processes are in place with appropriate checks and balances to enable directors to discharge their responsibilities. Accordingly, information security must be treated in the same way as all the other components of corporate governance. This includes making information security a core part of executive and board responsibilities.

Critically, corporate governance requires proper checks and balances to be established in an organisation; consequently, these must be in place for all information security implementations. In order to achieve this, it is important to have the involvement of three key role players, namely information security professionals, ICT security auditors and regulatory officials (from now on these will be referred to collectively as the 'role players'). These three role players must ensure that any information security controls implemented are properly checked and evaluated against the organisation's strategic objectives and regulatory requirements.

While maintaining their individual independence, the three role players must work together to achieve their individual goals with a view to, as a collective, contributing positively to the overall information security of an organisation. Working together requires that each role player must clearly understand its individual role, as well the role of the other players at different points in an information security programme. In a nutshell, the role players must be aligned such that their involvement will deliver maximum value to the organisation. This alignment must be based on a common framework which is understood and accepted by all three role players.

This study proposes a South African Information Security Alignment (SAISA) framework to ensure the alignment of the role players in the implementation and evaluation of information security controls. The structure of the SAISA framework is based on that of the COBIT 4.1 (Control Objectives for Information and Related Technology). Hence, the SAISA framework comprises four domains, namely, Plan and Organise Information Security (PO-IS), Acquire and Implement Information Security (AI-IS), Deliver and Support Information Security (DS-IS) and Monitor and Evaluate Information Security (ME-IS).

The SAISA framework brings together the three role players with a view to assisting them to understand their respective roles, as well as those of the other role players, as they implement and evaluate information security controls. The framework is intended to improve cooperation among the role players by ensuring that they view each other as partners in this process. Through the life cycle structure it adopts, the SAISA framework provides an effective and efficient tool for rolling out an information security programme in an organisation.

Key words: information security professionals, ICT security auditors, regulatory officials, framework, role players, information security programme, corporate governance, IT governance, COBIT

Contents

List of figures

List of tables

Chapter 1

Introduction

1.1 Introduction

Information security has become a matter for consideration at the top level of organisations. This is as a result of the increasing risks inherent in, and the rising expenditure on, organisational resources for information security. This has been brought about by increasingly stringent regulations and growing liabilities in case of compromise of information (IT Governance Institute 2006). In order for information security to be visible to the top-level management of the organisation, it should form part of corporate governance through its integration into strategy, concept, design and implementation, as well as its operation (IT Governance Institute 2006). Corporate governance can be loosely described as involving the establishment of the structures and processes, accompanied by the appropriate checks and balances that enable directors to discharge their legal responsibilities (King 2009).

Good corporate governance prescribes that the overall corporation is to be transparent, with processes, checks and balances in place that ensure good financial reporting; therefore information security processes should display similar transparency (Loyd 2004). Key to this is the presence of clearly defined roles and responsibilities in the security administration process (Nanggroe 2011). These clearly defined roles and responsibilities are central to the concept of separation of duties, that is, that security is enhanced by the division of responsibilities in the production cycle (Nanggroe 2011, Tipton, Krause 2004). Accordingly, it is important that the individual roles and responsibilities of information security are clearly communicated and understood (Nanggroe 2011).

Information security professionals design, implement and maintain information security controls in an organisation (ISACA 2007). Such professionals are the first role players forming part of this study. Subsequently, the information security controls implemented in an organisation must be reviewed by an independent party in a form of an **ICT security auditor** (Loyd 2004). ICT security auditors form the second group of role players that are examined in this research. Consequently, the design and implementation of information security controls must be built on a solid understanding of the pertinent legal and regulatory requirements and restrictions (ISACA 2007). These regulatory requirements are overseen by a body of

regulatory officials that seeks compliance either on a voluntary or a mandatory basis, using a set of laws, rules, regulations or codes (King 2009). These regulatory officials form the third set of role players being examined in this study.

The three role players need to have a sound understanding of the various factors that have implications on information security. Critically, they need to bear in mind that information security, through corporate and IT governance, is the responsibility of both the executive and the board of an organisation. Accordingly, its evaluation must be elevated to the level of a business issue, rather than being regarded as merely a technical issue (and left to the IT technicians). As a business issue, it should be dealt with at all levels of the organisation (Von Solms 2006). This also requires that information security related activities should be treated in the same way as any other business-critical activity, that is, they must be thoroughly planned for, effectively executed and constantly monitored at the highest levels of the organisation (IT Governance Institute 2008). Proper management of information security involves adequate risk management, reporting and accountability (IT Governance Institute 2006).

Information security is a complex subject and implementing the controls involved in an organisation is not an easy exercise (ISACA 2009a, Trcek 2003, Von Solms, Von Solms 2004). Information security is a combination of technical, administrative and physical controls (Cunningham et al. 2005, Pfleeger, Pfleeger 2002). Technical controls include controls such as firewalls, antivirus programs and encryption. Administrative controls, on the other hand, include those such as policies, standards and user awareness, while physical controls include controls such as biometrics and access cards (Harris 2005).

Information security is, therefore, a multidimensional discipline (Von Solms 2001). Other than the corporate governance dimension, it also includes the legal, the measurement/metrics (compliance monitoring/real time audit) and the audit dimensions (Von Solms 2001). Each role player thus plays a part in each of the information security dimensions in a greater or lesser way.

Implementing information security controls requires resources in the form of financial, human and time, among others (Anderson, Choobineh 2008, Powner 2005). These resources are of a limited nature and, as a result, information security programmes must compete with

other business requirements for the same resources. Some of the business requirements are for income generation and, understandably, business executives may be biased towards activities that have the potential to improve the organisation's bottom line (Anderson, Choobineh 2008). However, the organisation may pay a huge price for ignoring information security; for example, if the organisation were to become a victim of a security breach, it might suffer financial loss, theft or damage to information, loss of image and reputation, as well as legal action (Hermason, Hill & Ivancevich 2000, Humphreys 2008).

It is important for executives and boards of directors to understand and appreciate the importance of information security. Accordingly, information security professionals need to help executives understand this importance. Key to this is for information security professionals to have good communication skills that enable them to communicate at all levels of the organisation (Tipton, Krause 2004). Nevertheless, despite the fact that communication is an important tool, it is in no way the only skill that information security officials should possess. Other important skills include technical skills, business knowledge, legal awareness and organisational processes (Sundt 2006). This therefore highlights how complex the work of the information security professional is.

Similar challenges are experienced by ICT security auditors. These professionals are the 'eyes and ears' of management, in that they measure and report on the information security position of the organisation (Wright 2008). ICT security auditors need to understand the environment (internal control model of the organisation) being audited in order to be able to voice opinions that are relevant and useful to the organisation (ISACA 2008a). Once the internal control model has been established, the auditor will be in a better position to proceed with the test for compliance to the model (ISACA 2008a).

In order for auditors to establish an internal control model, they must interview the managers of the organisation and go through written descriptions and flowcharts of the organisation's systems and processes (Bailey 1979). For large corporations, information received by the auditor, while trying to establish and identify any weakness in the model, may be too much (Bailey 1979). Furthermore, as enterprise systems (to be audited) are large, complex and physically distributed (Zimmermann 2009), in order for an auditor to be

able to understand, comprehend and audit these complex models and systems they must possess appropriate business skills and relevant experience (Zimmermann 2009).

The third role player that this research examines is the regulatory officials (regulators). Regulators are concerned about the extent to which the organisation complies with regulatory requirements. These requirements could be the laws of the country in which the organisation is operating, for example licensing issues, or could be industry-specific regulations applicable to the industry in which the organisation is operating, such as codes, practices and standards. Apart from financial risk and other corporate risks, regulators are specifically concerned about operational and systemic risk, within which technology risk and information security issues reside (IT Governance Institute 2006). As such, information technology is the foundation and facilitator of the operational risk management framework (IT Governance Institute 2007b).

Effective oversight of compliance requires the establishment of a review process to ensure compliance with laws, regulations and contractual requirements. This process includes identifying compliance requirements, optimising and evaluating the response, obtaining assurance that the requirements have been complied with and, finally, integrating IT compliance reporting with the rest of the business (Liell-Cook, Graham & Hill 2009).

Clearly the three role players have a huge role play in the implementation and evaluation of information security controls. While the information security professionals must play a role of implementing controls, ICT security auditors are there to provide independent review of the implemented controls. Regulatory officials exist to ensure that the applicable laws and regulations with regard to information security are complied with.

For each role player to effectively and efficient execute their responsibilities it is important that they must work together, not against each other. One way of fostering the cooperation among the role players is the use of a common reference with regard to implementation and evaluation of information security controls. Such a framework must guide the three role players in terms of the implementation and evaluation of the information security controls in an organisation. The adoption of a framework contributes to the quick implementation of good practices and avoids lengthy delays in creating and agreeing on new approaches that simply reinvent the wheel (IT Governance Institute 2008a). A framework also helps to ensure

that the implementers of information security controls (information security professionals) and the evaluators/assessors (ICT security auditors and regulatory officials) are better aligned.

1.2 Why The Three Role Players Were Chosen For This Study?

The individuals delegated the responsibility for implementing and maintaining security by senior management are information security professionals (Nanggroe 2011). They therefore have a very important role to play in ensuring that both the executive management and the board are able to discharge their duties pertaining to information security. According to a recent Frost and Sullivan research report, the top five most time-consuming activities for information security professionals include meeting regulatory compliance and auditing IT security compliance (Ayoub 2011). This therefore shows that regulatory compliance and IT security auditing are critical matters for information security professionals.

ICT security auditors have a crucial role to play in information security. They achieve this by conducting regular, independent audits and by providing reports to senior management on the effectiveness of security controls (Nanggroe 2011). In addition, they ascertain whether security policies, standards, guidelines, and procedures effectively comply with the company's stated security objectives (Nanggroe 2011). For these reasons information security professionals and ICT regulatory auditors were included for investigation in this study.

Adherence to the law and regulatory controls is the foundation or baseline upon which an information security programme must be built (Wright 2008). At a minimum, it is necessary to adhere to the requirements imposed by law on the organisation (Wright 2008). Compliance to legal and regulatory requirements by the organisation is not an option, but a critical part of the information security programme. It is, therefore, important for an organisation to identify a role that is responsible for reviewing the organisation's information security policies and standards in terms of legal and regulatory compliance and enforceability (Tipton, Krause 2004). In a recent survey conducted by the Information Systems Audit and Control Association (ISACA), regulatory compliance was identified as the

number one concern for information security professionals and auditors (ISACA 2011b). External regulatory officials can perform inspections on organisations to verify compliance with the applicable legal and regulatory requirements. The role of these regulatory officials can never be overstated; hence, they have been included in this study.

1.3 Problem statement

The three role players have a similar goal in mind, that is, to assist organisations in implementing the necessary information security controls and, as a result, protecting the organisation's information assets. This contributes to ensuring that the interests of the various organisational stakeholders (e.g. customers and shareholders) are properly protected. While the role players' ultimate goal may be the same, their roles and responsibilities are distinct and different.

Notwithstanding the difference in roles and responsibilities of the role players, the nature of their work requires them to interact with each other at various stages of the information security programme. The challenge, however, is the lack of alignment among them in relation to the implementation and evaluation of information security controls as each role player has its own approach and standards when implementing and evaluating information security controls (Tipton, Krause 2004, ISACA 2009a, National Computing Centre 2005).

It would appear that there are differences between what information security professionals implement and what ICT security auditors assess as they conduct their audits. This can be attributed to many challenges, including communication gaps, hidden checklists, and a failure to collaborate on control assessment and control improvement (National Computing Centre 2005). This, then, results in the wastage of resources (money and time) through disagreements and back-and-forth discussions regarding what information security professionals believe are the correct controls to be implemented versus the findings made by the ICT security auditors.

As part of implementing information security controls, organisations should also observe and incorporate the legal requirements applicable to their environment. This, however, comes with its own challenges. Since information security professionals are not legal experts

it is difficult for them to understand the "minutiae and vagueness" (Tipton, Krause 2004) of existing regulatory guidelines and the legal consequences of companies' failure to implement correct information controls (Tipton, Krause 2004). Secondly, the difficulty facing organisations is that few laws and regulations specify how compliance is to be achieved (Sundt 2006). The discretion is then left to organisations themselves in the way they to go about achieving compliance. Subsequently, in most cases, the way in which legal and regulatory requirements are met depends more on people and procedures than on technical controls (Sundt 2006). This implies that there could be misalignment between what information security professionals think are the right controls to comply with regulatory requirements and what regulatory officials expect.

To find a solution to the problem of misalignment among the role players in implementing and evaluating information security controls, a framework needs to be developed that will address the following research questions:

- How can interpretation problems experienced by the role players relating to the implementation and evaluation of information security controls be prevented?
- What prioritisation challenges are faced by the role players?
- What can be done to establish a solution/delivery/measurement-oriented approach to implement and evaluate information security controls?
- Are the roles of the three role players clearly defined and understood?

1. *How can interpretation problems experienced by the role players relating to the implementation and evaluation of information security controls be prevented?*

Often, what auditors discover when conducting their audits is disputed by information security professionals (Tipton, Krause 2004). While such information security professionals expend their resources trying to provide protection for information assets using various controls, ICT security auditors often find these controls to be inadequate. Similarly, this also applies to the regulatory authorities. Companies may put in place all the controls they think are necessary in order to meet the regulatory requirements only to find that the regulatory authorities are not satisfied with these controls (Sundt 2006).

Moreover, information security professionals are bombarded with information from independent consultants regarding what controls need to be put in place in order to comply with various requirements. Sometimes what such consultants recommend may not be in line with what the auditors and regulatory officials look for when doing their audits. This lack of alignment may be caused by different and inconsistent interpretations of various codes and laws by different role players. Such differences may also be attributed to individual experience, bias, choice and subjectivity, which then lead to disagreements among the role players in terms of what security controls should be put in place, as well as how those controls should be implemented (Tipton, Krause 2004).

2. *What prioritisation challenges are faced by the role players?*

Owing to the competition for limited resources, information security professionals find themselves having to make difficult decisions with regard to what controls to install first and which ones to put in later. This is usually decided through a prioritisation process. However, when auditors and regulatory officials assess the controls in the environment they just look at what controls have been implemented and which have not. Consequently, they do not take into account the fact that some controls may not have been implemented because they fall much lower down on the prioritisation list as a result of issues such as budget constraints (Business Software Alliance 2003, Courtney 1982)(Business Software Alliance 2003). One of the reasons for this is the lack of a framework for setting priorities, assigning tasks, getting started and monitoring implementation (Business Software Alliance 2003)**.**

3. *What can be done to establish a solution/delivery/measurement-oriented approach to implement and evaluate information security controls?*

The motivation behind implementing information security controls should not be to impress ICT security auditors or regulatory officials. If this is the case, the organisation may resort to simply implementing controls for the sake of satisfying the auditors and the regulators, without actually extracting or understanding the value provided by those controls – an approach that is ineffective and inefficient. Information security controls should be subject to appropriate scrutiny using a formal process to articulate and measure the benefits that the controls will provide to the business.

4. *Are the roles of the three role players clearly defined and understood?*

The roles of auditors (especially internal auditors) and certain regulators are sometimes not properly articulated. Comsec Ltd, a government agency responsible for information security for the state (South Africa) and its agencies, provides consulting (and implementation) services, while at the same time performing annual audits to verify that state organs comply with Comsec requirements. This approach may create the perception that auditors are not independent or objective during the audit process, especially if they conduct an audit on what they have implemented in or recommended to an organisation themselves.

In order to avoid issues related to duplication of efforts, it is critical that the three role players work together in implementing and evaluating information security controls. In support of this it should be noted that a 'silo' approach leads to inefficiencies and a number of disadvantages, including putting pressure on resources and a costly "throw-away and start again" approach (Pinder 2006).

1.4 Purpose of the study

The purpose of the study is to develop a framework that can be used by ICT security auditors, ICT regulatory officials and information security professionals to implement and assess information security controls within organisations in a uniform and consistent manner.

The purpose of the framework is twofold: firstly to ensure that ICT security auditors, information security professionals and ICT regulatory authorities understand their respective roles and responsibilities with regard to the implementation of security in compliance with various requirements. The second purpose of the framework is to help each role player understand the work of the other role players. This should, firstly, assist the role players to have intelligent dialogue when discussing information security related issues. Secondly, this understanding is crucial in reducing or identifying risks that have not been adequately addressed (Hermason, Hill & Ivancevich 2000).

The principle behind the framework is its simplicity and practicality, while at the same time it can be adapted to the specific needs of individual organisations. The framework seeks to

provide a common language and clear direction and guidance on how information security controls should be implemented and evaluated (COSO 2004a).

1.5 Research objectives

The objectives of the study are to

- identify areas of mutual understanding among the three role players regarding the implementation and evaluation of information security controls. These are areas of integration and synchronisation where the role players particularly agree with each other.
- identify the methodologies and tools each role player uses in the implementation and/or evaluation of information security controls
- bridge the gap between the controls that must be implemented by information security professionals and what ICT security auditors and regulatory officials look for when they evaluate the controls. This will ensure that each role player benefits from a better understanding of the terminology, techniques and work approach of the other role players.
- ensure alignment among the role players regarding what must be implemented by implementers (information security professionals) vis-à-vis what is evaluated by the evaluators (ICT security auditors and regulatory officials). This alignment must be established from the very beginning of the information security programme.
- establish the groundwork of a **framework** that can be used by the role players to implement and evaluate information security controls in South Africa

1.6 Limitations

This study seeks to establish an information security framework that is applicable to the South African environment. To this end, regulations and codes relating to information security that are not specifically applicable to the South African environment (e.g. Sarbanes-Oxley) will not form part of this study.

The framework to be developed will focus primarily on large enterprises. Typically, these are organisations that have 250 or more employees (Oldsman, Hallberg 2006). Small enterprises will not be explicitly covered because, it may be argued, they rarely establish a dedicated information security group/department owing to factors such as budget constraints and shortage of expertise (Eloff, Eloff 2005).

The study will be biased towards the financial and telecommunications industries. These are industries that are greatly affected by many stringent regulations (ISACA 2008a).

The three role players forming part of this study are not the only important role players in information security. There are many other important ones, including the board of directors, the executive management, senior and middle managers, and all other employees of the organisation (Von Solms, Von Solms 2006b). However, this study is limited to looking at information security professionals, ICT security auditors and regulatory officials, and thus the final framework to be derived will only be applicable to these three role players.

1.7 Significance of the study

The framework that will be the outcome of this research study is intended for use by the role players in the implementation and assessment of information security controls in South African organisations. It will help the role players understand what exactly is expected of them. Moreover, it will assist each role player in understanding what is expected of the other role players, which will help to minimise instances of ambiguities and issues around semantics.

The framework will play a crucial role in bringing about much-needed alignment among the three role players. This alignment will ensure that information security professionals do not view ICT auditors and regulatory officials as enemies who are looking to find something negative in their work. Instead, they should view them as partners in helping them to fulfil their main goal: ensuring effective information security in the organisation (Wright 2008). Similarly, this framework will assist in ensuring that the ICT auditors and regulatory officials do not approach the auditees with a view to finding only the negative aspects of their work;

they approach their work with the intention of helping auditees improve their controls to acceptable levels.

The alignment to be brought about by the framework seeks to minimise unnecessary debates among the role players. Instead, it will assist in ensuring that the role players understand each other's work. This will help to guarantee that the role players are able to reach conclusions or agreements quicker and will save the organisation resources (time and money) by having the role players spend more time implementing and assessing controls than on debates (finger-pointing) about the differences regarding the controls.

1.8 Methodology

The research methodology employed in this study is primarily of a phenomenological nature. This is also known as interpretivist research –the researcher gathers information and filters it, while involving him/herself in the study (Maphakela 2008). In this kind of research, subjectivity plays a role, with the researcher having to argue his/her interpretation of the research area and the proposed solution (Maphakela 2008).

The literature study will cover the following areas:

- The status of information security in South Africa. This includes the initiatives taking place in South Africa as well as the regulatory regime.
- Three key role players in the implementation of information security. The intention here is to also look at the methodologies, techniques and tools they use to execute their duties.
- Key challenges in the implementation and evaluation of information security controls.
- An overview of key current information security and related frameworks.

The data to be used in the literature study will be collected mainly from journal articles, conference papers, books, previous dissertations/theses and the web (internet) in general.

On conclusion of the literature study, a logical argumentation will be established which will lead to the creation of the SAISA framework.

1.9 Definitions of key terms

An **ICT security auditor** is an independent person within or outside the organisation who checks the status of information security (Wright 2008). ICT security auditing responsibilities involve providing independent evaluations of an organisation's policies, procedures, standards, measures and practices for safeguarding electronic information from loss, damage, unintended disclosure, or denial of availability (EDP Audit Committee 1995).

The **regulatory officials'** role is to ensure that the laws and other regulatory requirements are complied with. These officials can impose penalties and sanctions on the offending party in the event of a deviation from the regulatory requirements. One example of such a regulator is COMSEC Ltd, which is mandated to ensure that state organs comply with the COMSEC Act (Comsec 2009). In this study, however, the term *regulatory official* does not just refer to the external regulators; it also includes professionals such as legal counsels and ICT lawyers who have the legal expertise to interrogate information security controls in relation to the legal requirements. Compliance officers also fall into this category, as they have a responsibility to provide the organisation with guidance on legal, regulatory and contractual compliance (ISACA 2011a).

Information security professionals, also known as security practitioners or information security officers, are the individuals who develop and implement information security policies and standards within the organisation. The policies they develop must be in line with the regulatory requirements, while at the same time help organisations to meet their goals (ISO/IEC 27002 2007). **Information security** is the protection of information from a wide range of threats in order to ensure business continuity, minimise business risk, and maximise return on investment and business opportunities (ISO/IEC 27002 2007).

A **framework** is a broad overview, outline, or skeleton of interlinked items which supports a particular approach to a specific objective, and serves as a guide that can be modified as required by adding or deleting items (Business Dictionary 2009).

Role players in this study are regulatory officials, information security professionals and ICT security auditors.

1.10 Dissertation Layout

The layout of this dissertation is depicted on figure 1.1 below:

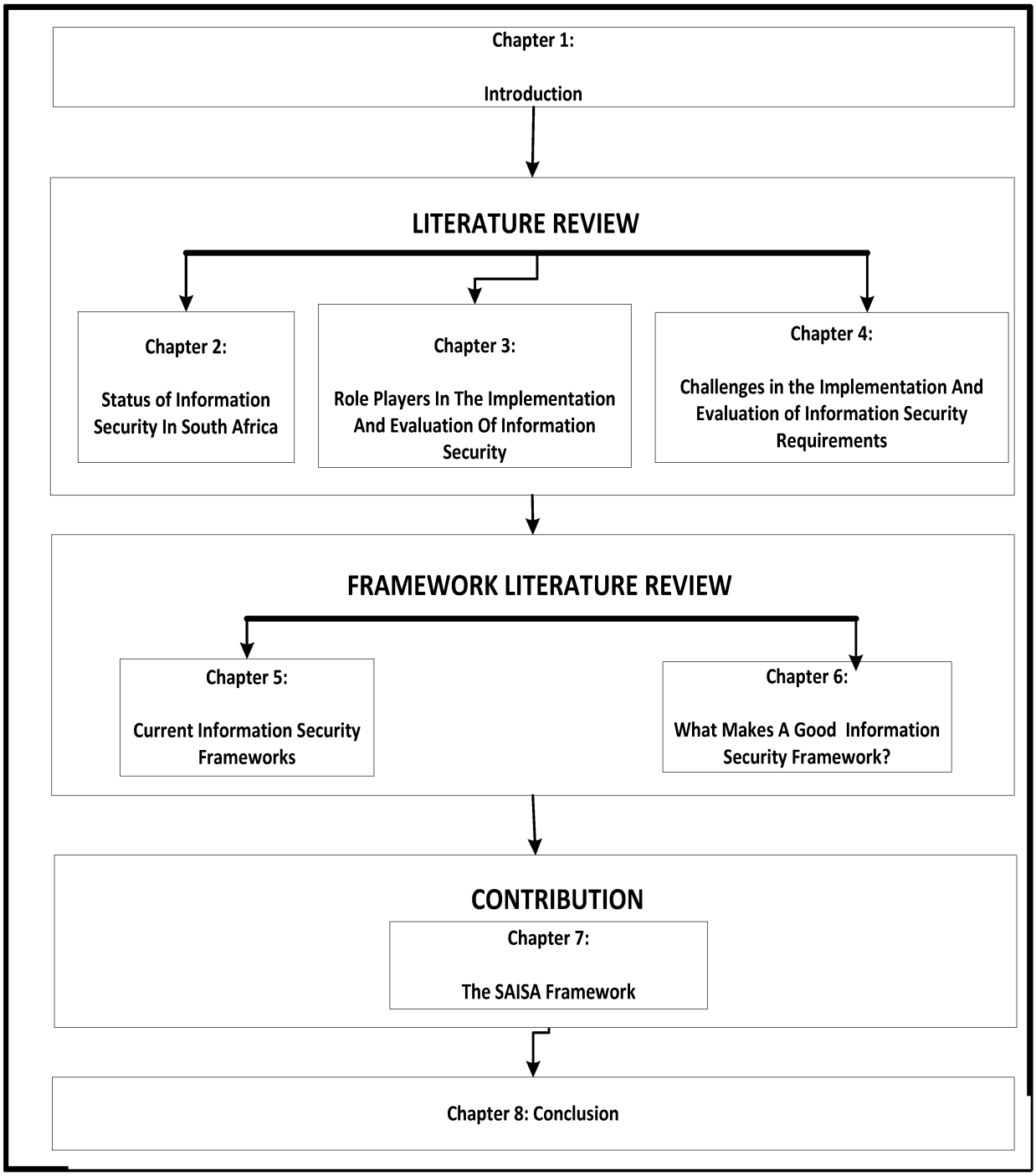


Figure 1.1 Dissertation Layout

Chapter 1 (Introduction): This chapter provides an outline of this research study. It introduces the study and the motivation behind it. It further defines the problem statement as well as the research questions underpinning the study. The key terms used in this study are defined in this chapter. It concludes with an overview of the remaining chapters.

Chapter 2 (Status of information security in South Africa): This chapter seeks to establish initiatives taken in South Africa (SA) with regard to information security. Areas to be covered in this chapter include activities initiated by the government and the private sector, as well as through public–private partnerships. Another area of interest will be the regulatory environment and this will include legislation passed by the South African government and the generic codes and standards affecting information security in South Africa. Focus will also fall on any other South African organisations that have come up with initiatives that have advanced the interests of the information security community. Establishing this status will be crucial in understanding the parameters within which the role players operate in terms of the implementation and evaluation of information security controls.

Chapter 3 (Role players in the implementation of information security): In this chapter the roles and responsibilities of each of the three role players (ICT security auditors, information security professionals and regulatory officials) are discussed in detail. The chapter dwells on the various approaches and methodologies employed by each role player as they go about implementing or assessing information security controls in organisations. Understanding the roles and responsibilities is critical in establishing the common areas and the areas of difference among these key role players regarding the implementation and evaluation of information security controls. Establishing this understanding is an important step towards the formulation of the new framework.

Chapter 4 (Challenges in implementation and evaluation of information security requirements): The primary purpose of this chapter is to look at the challenges specific to each role player as they implement or assess information security controls in an organisation. These challenges may emanate from the role player's profession itself or as a result of frustrations caused by other circumstances. The challenges presented by misalignments among the role players in the implementation and evaluation of information security controls will be studied in this chapter. Understanding these challenges will help

craft a framework that addresses these challenges with a view to creating a solution to them.

Chapter 5 (Current information security frameworks): This chapter takes the reader through a number of existing frameworks and standards that have an impact on information security. Each framework being studied is evaluated by highlighting the strengths and weaknesses of the framework.

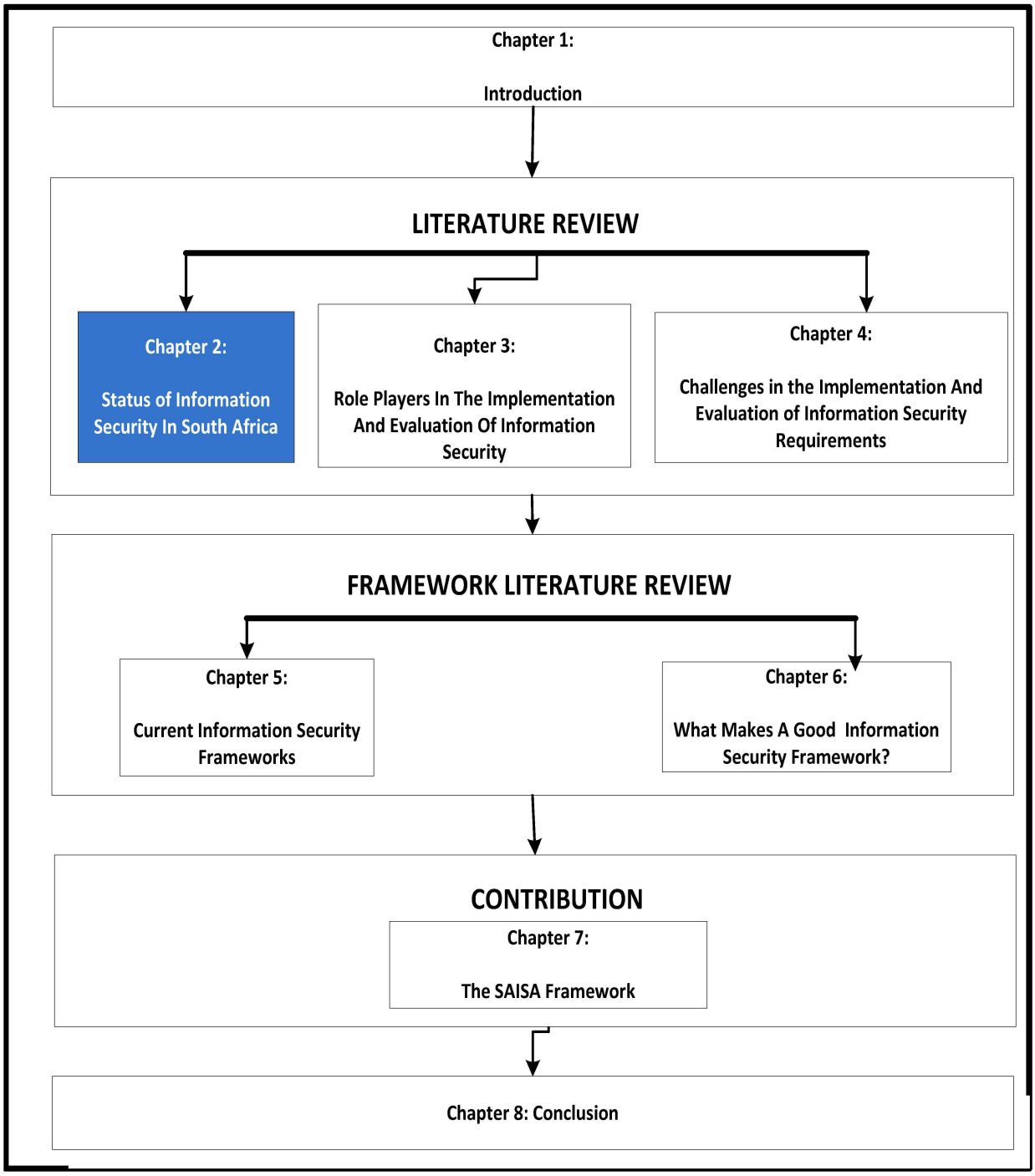
Chapter 6 (What makes a good framework?): This chapter focuses on the elements and attributes found in various frameworks. It also seeks to determine the common attributes among them so that what makes a good framework can be established. This information will inform the design and structure of the new framework.

Chapter 7 (The SAISA framework): The crux of this research study is presented in this chapter. Based on the research, a framework for implementing and evaluating information security controls is formulated for the role players. The framework is the actual deliverable that can then be applied in a real-world situation.

Chapter 9 (Conclusion): This chapter summarises the outcome of this research study. The reader is reminded of the initial objectives and then the outcome of the study is compared with those objectives to ascertain whether they have all been met. This chapter also proposes future work to be undertaken on the basis of this study.

Chapter 2

Status of Information Security in South Africa


Chapter 1:
Introduction
LITERATURE REVIEW
Chapter 2:
Status of Information Security In South Africa
Chapter 3:
Role Players In The Implementation And Evaluation Of Information Security
Chapter 4:
Challenges in the Implementation And Evaluation of Information Security Requirements
FRAMEWORK LITERATURE REVIEW
Chapter 5:
Current Information Security Frameworks
Chapter 6:
What Makes A Good Information Security Framework?
CONTRIBUTION
Chapter 7:
The SAISA Framework
Chapter 8: Conclusion

2.1 Introduction

Every organisation (private or public) relies on its information assets in order to prosper and survive (Mears, Von Solms 2004). This information is either in a transmitted mode or stored mode (Pfleeger, Pfleeger 2002). Subsequently, organisations are today conducting business in an interconnected and information-rich environment (Eloff, Eloff 2005). While the technologies and other media used to transmit and store information are useful in supplying business solutions, they also bring with them complex vulnerabilities (Eloff, Eloff 2005). Means of transmission vary from traditional methods such as post, courier, telephone, fax and video conferencing to modern methods such as email and the internet.

While information in the possession of the organisation can be used legitimately, it can also be used in ways that have the potential to harm the organisation in one way or another. The legitimate use of information assists organisations in sustaining and enhancing their business operations. This also involves the sharing of information with other stakeholders such as customers, shareholders, auditors and regulatory officials. Such sharing of information promotes transparency, which is a necessity for the organisation's corporate governance (King 2009). On the other hand, information can be used by unauthorised users who have ulterior motives for inflicting damage on the organisation. Unauthorised activities include hacking, information theft and denial of service attacks (Peltier, Peltier & Blackley 2005).

For information to be useful and reliable, it must be kept secure. Reliable information assists organisations to plan properly, use resources optimally and make other strategic decisions. Organisations must take measures to ensure that their information is protected and is reliable. If information is compromised it can have catastrophic results for organisations, for example corporate embarrassment, regulatory failure and/or financial loss (Williams 2007). Consequently, investment in the protection of information is not an option but a necessity.

National strategic institutions that rely on the accuracy and reliability of information, such as hospitals, airports, banks, water and electricity companies, could all be the target of attacks. If such institutions were to be victims of attacks, the country could be crippled. Owing to their strategic nature, such institutions could also be targets for terrorists who may want to destabilise the country and the economy. In response to 21st century pressures (e.g.

increased regulation, greater consumer choice, enhanced globalisation and terrorism), a holistic approach capable of recognising, preventing and reacting to threats to information assets is required (Williams 2007).

To ensure that a holistic approach to protecting the organisation's information assets and the national critical infrastructure is employed, public and private sector partnerships are very important in combating information security threats. South Africa has recognised this and has responded by embarking on initiatives to create and maintain public–private partnerships. These public–private partnerships have seen the creation of forums for knowledge sharing and collaboration. These include the Council for Scientific and Industrial Research, Business Against Crime South Africa, the South African Fraud Prevention Service and the South African Banking Risk Information Centre (FIC 2004). Public–private/partnerships have the potential to yield better results because such partnerships have led to great successes in preventing and combating threats such as cyber fraud (FIC 2004).

This chapter will cover the various information security threats facing the organisations in a South African environment. It looks at issues such as technological advancements, motives for attacks and economic effects of information security attacks. It discusses the various initiatives that have taken place in South Africa in response to the information security requirements.

2.2 Information security threats

Organisations use systems to create, store and transmit their information (Posthumus, Von Solms 2004). In order to preserve the security of information, certain attributes must be preserved during the life-cycle of information. These are the confidentiality, integrity and availability of information (ISO/IEC 27002 2007). Information can also have other properties such as authenticity, accountability, non-repudiation and reliability (ISO/IEC 27002 2007). Since the majority of information is created, stored and transmitted through systems such as computers and networks, it is vital that they (systems) are properly configured to ensure that information passing through them meets the requirements of information security.

Information security threats are influenced by many factors. The scope of this study will not cover all the threats to information security, but will highlight the most common ones.

Today, organisations are becoming increasingly dependent on **technology**. Technology has already become widely integrated into most organisations and can, therefore, be said to form the cornerstone of all information processing, storage and transmission (Posthumus, Von Solms 2004). Moreover, the proliferation of **mobile devices** in the modern organisation is staggering. With so many mobile devices in the enterprise, defending corporate data from leaks, either intentionally or via loss or theft of a device, is challenging. A 2011 report by Frost and Sullivan identified mobile devices as the second highest security concern for modern organisations (Ayoub 2011).

Information security threats are also influenced by the **motives** of those initiating attacks. Some of the motives are less serious (e.g. fun and games, thrills and bragging rights), while others are very serious (e.g. intelligence and financial gain) (Sagar 2005). Information security attacks can have serious economic effects (Symantec 2011), as nations and organisations use huge resources in combating information security threats and attacks.

In the 2011 report by Frost and Sullivan (Ayoub 2011), application vulnerabilities were identified as the top security threat concern. These vulnerabilities may be caused by various factors including the poor design of the system.

Critical infrastructure around the world has for some time been the target of cyber-related attacks for criminals, for political or other reasons. Hackers have access to a growing range of tools and techniques that could be used to engage in malicious activity directed against the computer-related components of critical infrastructure (Gordon 2003). Critical infrastructure consists of physical and information technology facilities, networks and assets (e.g. energy distribution networks, health services, essential utilities, transportation) which, if disrupted or destroyed, could seriously affect the health, safety, security and economic wellbeing of the country's residents. In addition, the effective functioning of industry and of government would be significantly affected.

The above-mentioned factors will now be examined in more detail.

2.2.1 Technology advancements

The advent of new technologies in the 21st century has brought about new risks owing to their ease of accessibility and their powerful nature. These technologies could be used in ways that seek to harm the targeted organisations/institutions and to destabilise them. Nowadays it is easy for anyone to go to the internet and find a hacking tool which can be used to cause damage to the target computer or the network. This kind of threat is usually referred to as 'script kiddie' owing to the low levels of programming, technical skills or knowledge required to conduct sophisticated attacks (Tipton, Krause 2004). Today, the problem has been exacerbated by the increasing usage of social media networks. For example, a tool was discovered that allows script kiddie to build botnets via Twitter (Jacoby 2010).

The advancement of technology continues to outpace the policy for law enforcement. Information security defence is still an immature field and the skills required to provide such defences are scarce and inadequate (Idefense 2008). There are also challenges of coordination among the agencies of different countries, which is further complicated by cases where there are conflicting national policies (e.g. on cyber crime), which are an advantage to cyber criminals who can choose to operate from geographic locations where penalties for some forms of cybercrime may not yet exist (Cashell et al. 2004).

The nature and sophistication of attacks are changing too. Far fewer attacks take down an organisation's entire IT system; instead, attacks now penetrate IT systems without impairing them, with their specific goal being to siphon off sensitive information over time without detection (Warner, Harris 2010). This means that if security professionals are expecting systems disruption as a sign that there is an attack underway, then they are likely to miss serious attacks which seek to steal information without causing visible disruptions.

2.2.2 Motives for attacks

The motive behind attacks has become more serious and such attacks are systematically planned to cause maximum damage to the victims. Such motives include the following (Brag 2003):

- *Military and intelligence.* These are attacks in which spies try to learn government secrets or disrupt government operations.
- *Business.* Attacks between competitors trying to hijack trade secrets.
- *Financial gain.* Attacks in which criminals try to trick banks or other financial institutions into sending them money or allocating them credit in an account against which they can make payments.
- *Terrorists.* Attacks in which politically motivated agents attempt to scare or harm the public by corrupting the computers of government, utilities or corporations.
- *Grudge.* Attacks in which disgruntled employees seek revenge on employers by wrecking their information systems.
- *Consumer fraud (identity theft).* Attacks in which con artists steal personally identifiable information about consumers (such as ID numbers or credit card numbers) so they can impersonate those consumers when purchasing goods or applying for credit or in which the con artists sell consumers bogus goods or services.

From these it is clear that information security threats affect every sphere of the economy, including both public and private industries, and their consequences are far reaching.

2.2.3 Economic effects of information security attacks

Information security attacks have negative effects on the organisation's financial position in one way or the other. Some attacks can have small effects on the organisation's business operations while others may have huge effects that may threaten its functioning and the survival. In addition, information security attacks have direct and indirect implications for the organisation's financial position and these include costs associated with putting preventative measures in place, the costs of remediation, the costs of bandwidth and equipment and the opportunity costs of congestion (Anderson, Choobineh 2008, International Telecommunication Union 2008).

While information security risks and threats are usually viewed in a negative light, it is important to note that the same threats also open up opportunities for other legal and legitimate businesses to thrive. Such businesses include anti-virus/anti-spam companies, security consultancy companies and network protection companies (firewalls and intrusion

detection vendors). Owing to the broad range of financial implications identified above, information security related issues, such as spam and malware, create mixed and sometimes conflicting incentives for stakeholders. Consequently, coherent responses to the problem are complicated (International Telecommunication Union 2008).

Studies have been undertaken to measure information security related attacks in monetary terms and the reports produced indicate the huge economic effects. For instance, a recent study by Norton in 2011 revealed the cost of cybercrime as US $114 billion annually (Symantec 2011). Malware incidents have also been cited as contributing to the increased costs of IT (Ponemon Institute 2010). This goes to show how serious the economic effects resulting from information security related incidents are (Cashell et al. 2004).

South Africa faces two major information security related crimes that have crippling economic effects. These are identity theft and phishing. There have been cases where users have been tricked into divulging their login information used to access their bank accounts. The financial institutions are, however, providing extra layers of security which include the use of security controls such as one time passwords (OTP) or random verification numbers (RVN) sent through cell phones and/or email in order to provide more security on certain transactions. While such measures provide an added layer of protection, it should be noted that this form of security has been compromised by syndicates that work with employees of mobile network operators to divert the OTPs or RVNs of the compromised bank accounts. A case in point is a R7 million scam that was allegedly perpetrated by a Vodacom employee. It is suspected that the Vodacom employee, working together with a syndicate, intercepted security SMSs (carrying OTPs and RVNs) issued to banking clients. Syndicate members would receive the messages and use them to conduct fraudulent online banking transactions (Dingle 2009).

The public sector has also not been spared information security related attacks. In recent years, South African government departments have become the victims of cybercrime which has cost the departments huge sums of money. Most of these crimes occur in the form of identity theft, phishing and the use of other hacking technologies such as spyware and keyloggers (Emigh 2005). For example, in June 2008, the KwaZulu-Natal government announced that cybercrime using sypware was committed in its departments of transport,

education, health, housing and agriculture. The value of the money swindled as a result of these crimes was more than R199 million (SAPA 2009). In another example, the Mpumalanga government lost a total of R5.5 million, which was stolen from its department of education Nedbank account after unauthorised access was gained to its basic management system (Mahlong 2009).

The occurrence of the information security attacks indicates that without proper controls the public and private sectors will continue losing money as a result of such attacks. The reported cases are in all likelihood the tip of the iceberg, as some companies are reluctant to report information security breaches owing to the reputational risks caused by bad publicity (Cashell et al. 2004). Despite this, some companies have adopted a transparent approach, for example, Zurich, an insurance company, issued a press statement after the organisation had lost one of its backup tapes containing client information (Renton 2009). Furthermore, criminals are being tried in South Africa's courts for crimes related to cybercrime although the rate of successful convictions is not clear at this stage.

2.2.4 Proliferation of portable devices

Owing to their perceived ease of use and the associated improved productivity, organisations have seen a proliferation of mobile devices in their environments. Mobile devices include laptops, tablets, cell phones and memory sticks. This has resulted in huge amounts of information, including emails, confidential documents and contact information, being commonly stored on these devices by employees. Confidential documents may contain information such as trade secrets, strategies and plans which are critical to the organisation's sustainability and survival. Moreover, disclosure of these documents to unauthorised users could leave an organisation facing many problems including lawsuits and loss of business and competitive advantage.

As a result of their mobile nature and small size, mobile devices can be easily misplaced or stolen. For example, in August 2008 a story broke about how the laptop belonging to the then Deputy Minister of Home Affairs (Malusi Gigaba) had landed up in a shop. Someone had dropped it there for recharging (Daily News Reporter 2008). The laptop had previously been reported lost. Fortunately for the deputy minister and the department, the shop's

owner became suspicious after receiving the laptop and was able to report it to the relevant officials. Based on this, some critical questions may be asked: What if the laptop had fallen on the wrong hands? What if the laptop had contained sensitive information about the country? Such questions indicate that, without sufficiently applied security controls, mobile devices pose serious risks.

Adding to the problem of the risks associated with mobile devices is the issue of mobile networking sites. Social networking sites have become very popular avenues for people to communicate with family, friends and colleagues from around the corner or across the globe. While there can be benefits from the collaborative, distributed approaches promoted by the responsible use of social networking sites, there are information security and privacy concerns associated with such sites (MS-ISAC 2010). Subsequently, the data suggest that an increasing volume of cybercrime is being directed at internet users on social networking sites (Reitlerlaw 2010).

With so many laws and regulations pertaining to the protection of information and privacy requirements, it is becoming increasingly necessary to enforce information security controls on mobile devices. Accordingly, all mobile devices now need to be considered **enterprise mobile workstations** (Hoffman 2007)**.** As such, they need to be treated as if they are 'mobile' workstations and must contain the very same protections (and more) that are afforded to LAN-based desktop workstations. Mobile devices are on the front line and they require in-depth protection— not providing it may have fatal consequences (Hoffman 2007).

2.2.5 Vulnerabilities of physical controls for information

The mistake that is usually made by information security professionals is to focus on information stored only on information systems and to pay less attention to information stored in other mediums. The most often neglected form of information is the one in physical format. Most critical infrastructure systems (although of a physical nature) rely heavily on information and process control systems for management and for functioning properly.

Information and process control systems play a crucial role in ensuring the stability of critical infrastructure. For example, the oil and gas industries use them to control flow in pipelines and refinery production; the electric power industry uses them to optimise power generation capacity and delivery; chemical plants depend on them for managing formulations and ensuring efficient production; water treatment systems rely on them for purification and delivery (Wybourne, Austin & Palmer 2009). There is a great deal of other infrastructure that could be added to this list, including air traffic control, transportation systems, nuclear power, as well as healthcare-related technologies such as embedded medical devices.

Critical information and process control systems consist of computers and the networks that interconnect them, as well as the sensors and actuators that physically monitor and control the processes. When first introduced in the late 1960s, process control systems were a collection of special-purpose computers and sensors on closed, often proprietary, local networks (Wybourne, Austin & Palmer 2009). As such, these early systems were relatively easy to protect from electronic intrusion and sabotage. However, as technology has evolved and process control systems have been developed to achieve better control, operational efficiency and audit capabilities, the security situation has changed. The internet, a cost-effective and easily available means to connect systems, has been a significant contributing factor in this change (Wybourne, Austin & Palmer 2009).

The security challenges associated with process control systems must be met within the framework of two key attributes: first, the systems must operate in real time, which limits any latent time available for security-related processing; secondly, the systems ideally should be uninterruptible but at least be able to recover rapidly and safely after an information security related disruption (Wybourne, Austin & Palmer 2009). An additional challenge is that process control systems often incorporate legacy components that have little built-in security.

Besides the fact that the physical critical infrastructure depend on information systems, there are other physical mediums that keep information. These include information on physical documents (e.g. books, meeting minutes and strategy documents) and some written on boards (discussion boards – someone may peep through the window and see

what is written on the board, which could be of a confidential nature) (ISO/IEC 27002 2007). The other information medium, which is rather difficult to protect, is the one in oral form and kept in people's memories. Once people have been exposed to sensitive information, it could take just one conversation with a colleague to reveal privileged information. Some companies and institutions rely on having their employees sign non-disclosure or confidentiality agreements, which act as one preventative measure, but such practices do not fully eliminate the risk.

2.2.6 Poorly designed systems

Poorly designed systems pose a great threat to the overall functioning of the final system. As has been noted above, most of the critical infrastructure systems are dependent on information and control process systems. If such systems were to be successfully attacked the country could find itself at a standstill. Systems that do not incorporate security from the design and implementation stages are more prone to successful attacks. Furthermore, the implications of such attacks are far wider than the system that is successfully attacked.

There are two ways of ensuring that security is not neglected during the design and implementation of the system: firstly, security should be made a consideration throughout the software development lifecycle and, secondly, it is important that the users and developers of those computer systems have security built into their understanding and use of the systems. People trained to understand the importance of security are far more likely to follow security guidelines and to strive to improve and streamline them (Wybourne, Austin & Palmer 2009).

This section has indicated how complex and challenging the area of information security has become. Combating threats and attacks requires adequate investment in information security controls.

2.3 Initiatives affecting information security in South Africa

South Africa has realised the importance of information security. This realisation has resulted in different initiatives being undertaken to address information security needs. There are many initiatives undertaken within the country to this effect, not all of which can be discussed as part of this study. The focus in this study is on the initiatives affecting the financial and the telecommunications environment (towards which this study is inclined). The initiatives include the passing of the legislation and drafting of Bills such as the following:

- Electronic Communications and Transactions Act of 2002
- Regulation of Interception of Communication and Provision of Communication-related Act of 2002
- Protection of Personal Information Bill
- The Promotion of Access to Information Act of 2000
- Financial Intelligence Centre Act of 2001
- Electronic Communications Security (Pty) Ltd Act of 2002

The initiatives undertaken have also included public–private partnerships as well as those spear headed by private organisations. These initiatives, attractive to information security professionals and ICT security auditors, have contributed positively in addressing information security threats and risks in South Africa. Many of these initiatives have impact on financial and telecommunications industries. The following initiatives have been identified as playing a key role with regard to information security in South Africa:

- The Council for Scientific and Industrial Research (CSIR)
- Business Against Crime South Africa (BAC)
- The South African Fraud Prevention Service (SAFPS)
- South African Banking Risk Information Centre (SABRIC)
- Information Security Group of Africa (ISG Africa)
- ISACA South Africa Chapter

- Information Security For South Africa (ISSA)
- Annual ITWeb Security Summit
- Auditing Firms

The above mentioned initiatives, Acts, Bills and public–private collaborations all have implications for information security in one way or another. These will be briefly discussed below.

2.3.1 Electronic Communications and Transactions Act (ECT Act), 2002

The Electronic Communications and Transactions Act (ECT Act) became law in 2002, addressing a number of issues related to electronic communications. The issues pertaining to information security that this Act specifically addresses include legal certainty, security, protection of individuals and illegal activities and enforcement (Michalson, Hughes 2005). As such, the Act recognises the importance of information security and offers protection to consumers particularly with regard to the release of their personal information.

2.3.2 Regulation of Interception of Communication Act, 2002

The purpose of the Regulation of Interception of Communication Act (RICA) is to allow enforcement agencies to intercept communication to investigate or directly prevent serious crime (De Wet 2003). This is critical because, with the technological advancement that is currently taking place, such technologies are sometimes used to commit crimes (especially against the communication infrastructure). This Act affects institutions such as internet service providers (ISPs) and telecommunications operators because they should be able to provide interception services when required by law enforcement agencies.

In drafting RICA, considerable care was taken to ensure that the two competing rights – privacy and security – are properly balanced and not infringed unreasonably. This is because once there is a system in place that enables the monitoring and interception of communication the temptation for abuse begins (De Wet 2003).

2.3.3 Protection of Personal Information Bill

The purpose of this Bill is to ensure the protection and release of personal information. Under this Act all businesses are required to provide legal protection for a person, employee or client when their personal information is collected, stored or used by another party (Deloitte 2011).

The Bill seeks to protect the public from the involuntary release of personal information. In other words, the use of personal information, which has been provided voluntarily, by an individual for any other purpose than that for which it was originally provided, without the individual's consent, would be illegal and would be an offence under the Act (Deloitte 2011).

2.3.4 The Promotion of Access to Information Act (PAIA)

The Promotion of Access to Information Act (PAIA) gives every person in South Africa the right of access to information held by the state and other persons and institutions. This means anyone can request access to information held by public bodies, as well as a natural or juristic person (SAHRC 2009).

This Act contains penal provisions for the intentional and fraudulent concealment or falsification of records and provides that a person acting in such a manner is guilty of an offence and liable for a fine or imprisonment for a period not exceeding two years (Internet Service Providers' Association 2007). This therefore means that if the information security procedures in an institution are not sound, such that the integrity and availability of its information is compromised, the affected institution could be liable for a fine or imprisonment under this Act.

2.3.5 Financial Intelligence Centre Act, 2001 (FICA)

The Financial Intelligence Centre Act (FICA) was established to combat money-laundering activities and the financing of terrorist and related activities and to impose certain duties on institutions and other persons who might be used for money-laundering purposes and the financing of terrorist and related activities (FIC 2004). This Act mainly affects financial

institutions such as banks and insurance companies. However, it also affects estate agencies which can be used for money-laundering purposes.

2.3.6 Electronic Communications Security (Pty) Ltd Act, 2002

The purpose of the Electronic Communications Security (Pty) Ltd (COMSEC) Act was the establishment of COMSEC (Pty) Ltd as an institutional authority to, among other things, identify and protect critical infrastructure; and to protect and secure critical electronic communications of the organs of state against unauthorised access in the form of technical, electronic or any other related threats (Padayachie 2008).

The company, in concurrence with the National Intelligence Agency, provides verification services for the electronic communications security systems, products and services used by the state (Comsec 2009).

2.3.7 King III

While the previous King report, King ll, indirectly addressed some information security needs, the latest report (King III) looks specifically at IT security ("information security") as one of the critical areas a company's board of directors must pay attention to as part of IT governance. The report recommends that the board must consider the importance of and need for IT security because, among other things, IT security contributes to enabling the business strategy, sustaining normal operations and meeting compliance requirements (King 2009).

2.3.8 Minimum Information Security Standards (MISS)

The Minimum Information Security Standards (MISS) document was approved by the South African Cabinet as a national information security document in December 1996 (McKinley 2003). The MISS is a comprehensive security document dealing with various aspects of information security including applications, documents, communication and physical security measures.

2.3.9 The Council for Scientific and Industrial Research

The Council for Scientific and Industrial Research (CSIR) is embarking on a project that will focus on helping the country to put strategies in place to counter any information warfare that may be conducted against it (Africa 2009). This research was triggered by a spate of cyber attacks that were directed at Estonian websites over a period of three weeks (Africa 2009). It is expected that this research project will be especially valuable to the South African Defence Force (SANDF), as its findings will improve the Defence Force's capabilities to protect the country against threats such as cyber attacks.

2.3.10 Business Against Crime South Africa (BAC)

Business Against Crime South Africa (BAC), a non-governmental organisation, was formed in order to combat crime using public–private partnerships (Stavrou 2002). BAC focuses substantially on commercial crime involving the use of IT systems. BAC provides support in combating these crimes through the provision of specialised training for detectives and court investigators.

2.3.11 The South African Fraud Prevention Service (SAFPS)

The South African Fraud Prevention Service (SAFPS) was formed in 2000 and started its operations in July 2001. The role of the SAFPS is to assist in the fight against impersonation and identity theft (SAFPS 2009). Its primary objective is to provide fraud prevention data-sharing services across all sectors of South African businesses. According to the SAFPS, their service has contributed to South Africa's economy and business through the prevention of more than R3 billion in attempted fraud (SAFPS 2009). Such efforts are clearly yielding positive results in combating e-crime.

2.3.12 South African Banking Risk Information Centre (SABRIC)

South African Banking Risk Information Centre (SABRIC) was created by The Banking Association of South Africa to provide intelligence support to banks against crime including e-crime. Its key stakeholders are the South African banks. SABRIC works on one key business

principle: detect, prevent and reduce organised crime in the banking industry through effective public–private partnerships (SABRIC 2009).

2.3.13 Information Security Group of Africa (ISG Africa)

Information Security Group of Africa (ISG Africa) is a non-profit organisation formed in 2005. It was created in response to the increase of IT security compromises and cyber crime in South Africa and the rest of the African continent (ISG-AFRICA 2012). Its major activities are to raise executive awareness and assist organisations with the broad range of information risks facing the African continent (ISG-AFRICA 2012).

ISG Africa consists of security professionals from corporate, government and IT. It provides the mechanism for regular exchange of information security knowledge (ISG-AFRICA 2012). It facilitates networking within the community whilst raising awareness of vulnerabilities and global threats in the African context. The Group has played a pivotal role in raising the profile of information security in South Africa and Africa (ISG-AFRICA 2012).

2.3.14 ISACA South Africa Chapter

The ISACA South Africa Chapter's mission is to promote the assurance, security and governance of information systems (IS) in South Africa (ISACA-SA 2012).

The chapter's main objectives are (ISACA-SA 2012):

- To promote the education of, and help expand the knowledge and skills of its members in the interrelated fields of auditing, quality assurance, security, IS audit and control, and IT governance.
- To encourage an open exchange of IS audit and control, quality assurance, and security techniques, approaches, and problem solving by its members.
- To promote adequate communication to keep members abreast of current events in IS audit and control, quality assurance, and security fields that can be of benefit to them and their employers.

- To communicate to management, auditors, universities, and to IS professionals the importance of establishing controls necessary to ensure the effective organization and utilisation of IT resources.
- To promote the Association's professional certifications.

2.3.15 Information Security For South Africa (ISSA)

Information Security for South Africa (ISSA) is the annual conference for the information security community established in 2001. Since 2010, ISSA is co-sponsored by the IEEE Systems, Man and Cybernetics Society (SMCS) Chapter (a chapter of the IEEE South Africa Section) (ISSA 2012). The annual ISSA conference continues to be recognised as a platform for professionals from industry as well as researchers to share their knowledge, experience and research results in the field of information security on a South African, but also on an international level (ISSA 2012).

2.3.16 Annual ITWeb Security Summit

The annual security summit, hosted by ITWeb, is the meeting place for IT and information security professionals, industry experts, analysts and solutions providers (ITWeb 2012). It is targeted to personnel operating within information security industry.

2.3.17 Auditing Firms

The auditing firms such as PWC, Delloite, KPMG, SizweNtsalubaGobodo and Ernest & Young also have a particular focus in information security in a form of auditing and consulting in South Africa. They play a key role by advising their clients on matters concerning information security.

2.4 Conclusion

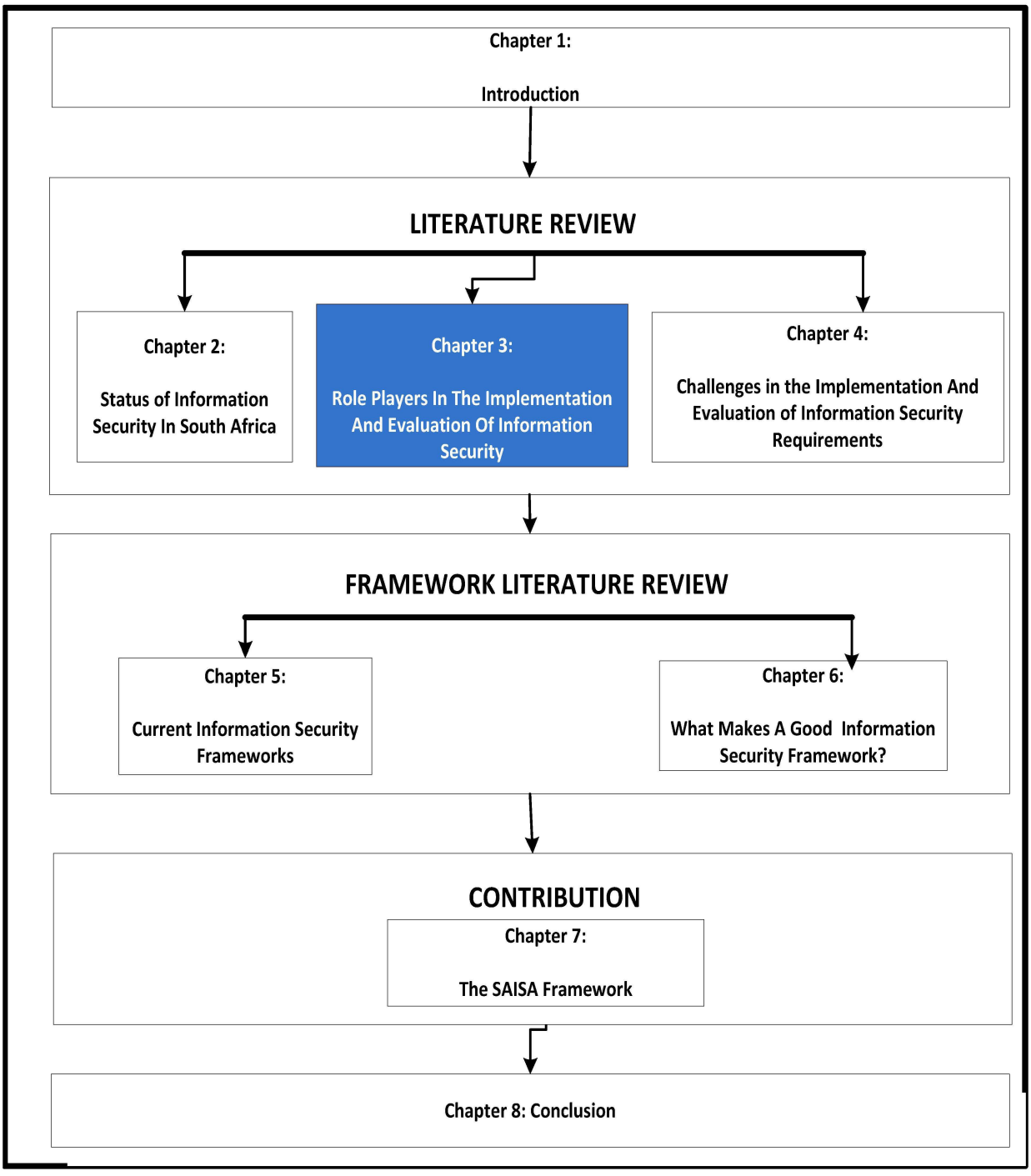
South African organisations, like their international counterparts, are facing various information security related risks as a result of their high dependency on their information assets and the systems that process them. Information security threats emanate from

various sources, such as cyber terrorism, phishing, hacking, denial of service attacks and identity thefts. Consequently, if no proper controls are put in place to address information security risks, the organisations could pay the price. To address this, South Africa has embarked on various initiatives that have seen the creation of legislation and codes such as King III. These have been complemented by the establishment of public–private partnerships that go a long way in combating information security related risks.

Information security controls are broadly divided into two categories. These are technical controls (e.g. firewalls, antivirus) and non-technical controls (e.g. policies, user awareness). The controls that are implemented are based on the internal requirements (e.g. business strategy) and the external requirements (e.g. industry codes and regulatory codes). To implement and evaluate the information security controls requires the skills and the involvement of key role players. The next chapter will discuss the key role players in the implementation and evaluation of information security controls.

Chapter 3

Role Players in the Implementation and Evaluation of Information Security


Chapter 1:
Introduction
LITERATURE REVIEW
Chapter 2:
Status of Information Security In South Africa
Chapter 3:
Role Players In The Implementation And Evaluation Of Information Security
Chapter 4:
Challenges in the Implementation And Evaluation of Information Security Requirements
FRAMEWORK LITERATURE REVIEW
Chapter 5:
Current Information Security Frameworks
Chapter 6:
What Makes A Good Information Security Framework?
CONTRIBUTION
Chapter 7:
The SAISA Framework
Chapter 8: Conclusion

3.1 Introduction

Information security is one of the corporate governance requirements that must be implemented and maintained during the normal course of business operations. The reasons behind this include regulatory and legal requirements, the maintenance of a competitive edge for the business and the sustaining of the business operations (Hermason, Hill & Ivancevich 2000). This requires that information security to be made part of the internal controls that govern the processes, operations and transactions that constitute the life of the organisation (Manjak 2006).

As indicated in chapter 1, the implementation and evaluation of information security controls requires the maintenance of proper checks and balances in line with corporate governance principles. To this end, three role players were identified as being important in the implementation and evaluation of information security controls. These are information security professionals, ICT security auditors and regulatory officials. Each role player has a crucial role to play in ensuring that the proper checks and balances are maintained.

While information security professionals are mandated with implementing information security controls, their work must be checked and verified by ICT security auditors and regulatory officials.

The rest of the chapter will focus on the three role players with regard to the implementation and evaluation of information security. It will focus on each role player by looking at issues such as the nature of their role, their challenges, their industry standards and the various approaches they use to execute their responsibilities.

3.2 Information security professionals

For information security professionals to execute their duties successfully, they need to work with different levels of authority within an organisation. These levels range from board, executive management to user levels (Kritzinger, Smith 2008). Furthermore, information security professionals must communicate and work with other internal and external stakeholders such as the auditors and regulatory officials. It is, therefore, a necessity that

information security professionals possess the communication skills that enable them to communicate with users at different levels of an organisation, as well as external stakeholders (Tipton, Krause 2004).

In addition, it is critical for information security professionals to understand that there are three dimensions in the implementation of information security controls. The first dimension pertains to technical issues (e.g. encryption and firewalls) while the second pertains to non-technical issues also called administrative controls (e.g. security policies and legal aspects) (Kritzinger, Smith 2008). The third dimension is the physical dimension (e.g. biometric and access cards) (Cunningham et al. 2005, Pfleeger, Pfleeger 2002).

In order to implement the activities associated with security controls, information security officers can apply various methods and methodologies. However, before the methodologies for implementing security can be applied, a security plan needs to be put in place. This plan must be drawn up on the basis of the outcome of a risk analysis exercise (Von Solms, Von Solms 2004). This approach ensures that the prioritisation of the security controls being put in place is in accordance with both the risks and the threats facing the organisation.

3.2.1 Role of information security professionals

Information security professionals are tasked with protecting the organisation's information assets, while ensuring that the controls put in place are in line with the organisation's strategic goals. The role of information security professionals is steadily changing: they are now responsible for the security of many facets of an organisation, including regulatory compliance, legal compliance, data security and access control (Ayoub 2011). Accordingly, information security professionals must find a balance between implementing the right controls in the organisation's environment while positively contributing to the organisation's goals. If poorly selected controls are imposed on users and systems, security may be viewed as a hindrance to the organisation's objectives (Hansche, Berti & Hare 2004).

For an information security professional to make a positive contribution to the organisational goals, a good understanding of the organisation's strategy is critical. This requires such professionals to be able to read and understand high-level business strategy and be able to translate the strategy into tangible technical and administrative security

controls. Information security is an area that is constantly changing and thus requires methods and solutions that ensure adaptations to new and ever-changing information security threats, countermeasures and the global business landscape (Dlamini, Eloff & Hone 2009). However, the new emphasis is on understanding the broader security risks so that security controls can address these risks (Williams 2007). It then becomes imperative that, as the business evolves, so must the information security controls.

3.2.2 Approaches in the implementation of information security

Depending on the culture and capability of the organisation, different approaches can be used in the implementation of information security controls within an organisation. This does, however, require that the organisation adopt certain principles that assist in the advancement of information security objectives. From a systems and applications point of view, three major principles are applicable (Julisch et al. 2011):

- *Defence in depth* – never relying on one control alone
- *Automation* – seeking to automate controls as much as possible
- *Fail-safe* – controls that break should default to a state that protects assets even though this may reduce usability or performance.

Information security professionals need to assess the environment and implement controls suitable for the organisation. However, one of the generally accepted approaches in implementing security involves identifying what must be protected, determining what it should be protected from, determining the likelihood of the threats, implementing controls that can protect the assets in a cost-effective manner and having the means to continually review the process and apply corrective measures or improvements where weaknesses are identified (Fites, Kratz & Brebner 1988). This approach will now be discussed briefly below.

(1) Identifying what must be protected

Information security professionals must, firstly, identify which information assets of the organisation have to be protected, the location of the information and in what form (physical or electronic) it exists. Executives make use of such information on a daily basis to make decisions that seek to bring the organisation closer to its goals. To make these

decisions, executives need information that is kept confidential and accurate, as well as available in a timely manner (Posthumus, Von Solms 2004).

Information security professionals need the involvement and cooperation of the business in identifying the information assets that need protection. Ultimately, these information assets belong to the business and, as such, the business must be in a position to know what information assets need protection.

(2) Determining what information assets should be protected from

Once information assets have been identified, the threats to these assets must be identified. A threat is an event that has the potential to cause loss or harm to computing resources such as hardware, software, data or communications networks (Pfleeger, Pfleeger 2002). Consequently, threats applicable to the processing system in question can be identified on the basis of the vulnerabilities within the information processing system. For a threat to cause damage to the information asset, it needs to exploit its vulnerability.

Threats come in three forms (Chaula, Yngstrom & Kowalski 2005):

- *Natural phenomena (act of God).* These include natural disasters such as volcanic eruptions and floods. They also include manmade catastrophes such as terrorism and power outages.
- *Technical nature (system malfunction).* Such threats exist as a result of organisations' dependence on IT systems. Examples include hardware and software defects, viruses and buffer overflow.
- *Human activities.* Humans can cause damage to the organisation's information assets either accidentally or maliciously.

(3) Determining the likelihood of the threats

Threats are not all equal. Some threats are more likely to occur and cause harm than others. This implies that threats should be rated according to their likelihood of occurrence. In line with this activity, the impact of each threat causing harm must be identified. For the purposes of addressing the threats, it is important that threats with a high likelihood of

causing harm and with a high resultant impact must be on top of the list. This exercise helps in terms of the prioritisation of controls.

(4) Implementation of controls to protect the assets in a cost-effective manner

The cost of implementing security controls must be commensurate with the value of the information asset being protected. This is to ensure that the controls being put in place do not result in over or under protection of information assets.

Since organisations do not have unlimited budgets, information security professionals are sometimes faced with challenges in obtaining the funding required for implementing security controls. The professionals must compete with other business units in the organisation in obtaining approval for their budgets. In order to convince senior management successfully, the budget requirements for information security should be aligned with the vision and mission statements, the business goals, the legal obligations, the overall risk appetite and the policy statements of the organisation (Dlamini, Eloff & Hone 2009).

(5) Continually review the process and implement corrective measures or improvements where weaknesses are identified

As circumstances change it becomes necessary to review the effectiveness of the controls put in place and to identify any gaps. Over time, some information may lose value and therefore require less and cheaper controls. The opposite is also true; some information may gain value over time thereby requiring stronger controls than initially implemented.

3.2.3 Information security programme

Once information security professionals know what information assets there are to protect, where they are located and in what form, an information security programme must be formulated. An information security programme should cover aspects such as strategies (prevention, detection, verification and response), tools, processes, people, roles and dimensions (governance, operations, architecture) (Onsett International Corporation 2001). These must be underpinned by the items that form the foundation of the information security programme, which include information security policy.

A typical information security programme would look like the one depicted in the diagram below:

Figure 3.1 Information security programme (Lilley 2009)

The above figure shows that the first step in the implementation of information security is the creation of a *security policy* and the approval thereof. A security policy acts as a blueprint for an organisation's security programme and provides the foundation on which to build such as programme (Harris 2005). A good security policy should incorporate both the users' needs for accurate and reliable information, as well as the business's needs for achieving its strategic objectives (Höne, Eloff 2002). This approach helps in that it encourages users to buy in to the security policy, while at the same time meeting the organisation's strategic goals. Moreover, a security policy must take into account the legislative, statutory and regulatory requirements the organisation must fulfil as part of its operations. In short, a security policy is the primary embodiment of organisational strategy, guiding the decisions made by users, administrators and managers, and informing those individuals of their security responsibilities (FFIEC 2006).

Once the security policy has been established, the next step is the formalisation of *responsibilities* in the area of security. When defining the responsibilities of security, principles for the segregation of duties must be enforced. Accordingly, the security policy must define responsibilities at the highest level.

Further, *security guidelines and standards* that support the security policy must be developed. As these items are developed, the security programme increases in granularity by developing baselines and configurations for the chosen controls and methods (Harris 2005).

Once the baseline in the form of a security policy, security and responsibilities, security standards and guidelines has been established, the next blocks of the security programme become more technical and detailed. These include the establishment of security management processes, risk management, technical security architecture, detailed technical procedures and asset classifications. These items ensure the proper implementation of security requirements as defined in a security policy.

Policies, standards and other security initiatives need to be communicated to the users. To achieve this, *training and user awareness* campaigns must be undertaken to ensure that users understand their security responsibilities, as well as how to act when faced with various security situations. In the case of hacking, for example, although technical solutions may be implemented in an organisation, if users are not vigilant in their activities hackers can count on their ignorance and exploit that weakness. Users must be encouraged to be constantly vigilant in order to ensure that they do not forget their security responsibilities. This promotes the responsible use of computers within organisations and minimises the risk of unauthorised access and irresponsible behaviour (Mears, Von Solms 2004).

Finally, a security programme must have the means and facilities for *reporting* the success and failures of established security programmes. Moreover, its reporting facility must be able to identify security violations and breaches. Good information security reports assist management to understand the organisation's security position and empower management to make informed decisions regarding information security. Reporting also assists in the identification of security gaps and, as a result, ensures that information security professionals are able to beef up security in areas of concern. Based on the results of

reports, policies may be updated to keep abreast of information security trends occurring within an organisation.

The security programme is a living process; accordingly, it needs to be planned for, implemented, measured and updated as required. It is therefore essential that senior executive management buy in to any security programme.

3.2.4 What does business expect from information security?

Organisations create high-level strategies and visions to take them closer to their strategic goals. In terms of these strategies, the onus then falls on the each business unit within the organisation to establish and implement plans that contribute to the overall organisational strategy. Information security professionals should do the same.

In financial and telecommunications sectors, where many stringent regulations are imposed, IT security professionals are required to meet high expectations on an ongoing basis (ISACA 2008a). Such expectations emanate from four stakeholders: customers, regulators, management and shareholders. These stakeholder expectations include the following (Symantec 2008):

- *Customers.* Current and future customers demand flawless delivery of innovative services in the belief that their money is safe and their confidential information protected.

- *Regulators.* Regulators and the public require orderly markets and transactions, and rapid, transparent response to public concerns.

- *Management and shareholders.* These parties expect smooth operations, prudent management of IT and business risks, and fast, confident responses to growth, change or crisis.

It is clear that all the requirements expected of IT professionals relate directly to information security and, as such, information security professionals should be able to translate these into elements that have to be delivered in their own programmes. They need to identify and

apply the relevant controls to ensure that expectations are met from an information security perspective.

To assist the organisation in achieving the typical requirements as indicated above, some of the attributes expected of information security professionals include the following (Fitzgerald, Krause 2008):

- Can manage the creation and implementation of enterprise-wide solutions.
- Have a thorough understanding of the business. The security position must be tailored to the specific needs and risk appetites of the business.
- Are aware of regulatory/legal/privacy implications. Information security professionals need to understand the impact that these requirements have on the information security programmes they are implementing.
- Develop relationships, communicate and sell ideas effectively to senior management.
- Can apply a technology risk management approach. They must understand that information security is not a technology issue; it is a business issue.

The attributes listed above indicate that an information security professional must be someone who is able to think both at the strategic and the technical levels. In their plans, information security professionals should incorporate all the business requirements. The alignment of security plans with organisational plans is very important if security programmes are to be successful in an organisation.

3.3 ICT security auditors

The role of ICT security auditors is to provide independent assurance to the organisation that the controls implemented are indeed correctly implemented and that they serve the purpose they were designed for. Auditors must be independent of any influence, be it internal or external to the organisation. Corporate governance is formed by, among other things, internal audit, external audit, senior management and the board (Rose, Norman 2008). Auditors must report to the audit committee of the board of directors in order to avoid any conflict of interest (Chorafas 2008). Auditors are divided into two categories: internal auditors and external auditors.

3.3.1 Internal auditors

Internal auditors are meant to remain independent in order to provide objective assurance and consulting activities designed to add value and improve an organisation's operations. These auditors help the organisation to achieve its objectives through a systematic, disciplined approach to evaluating and improving the effectiveness of risk management control and governance processes (IIA 2010).

The scope of internal auditors is broad and spans many areas including the following (COSO 2004b):

- Internal control systems
- Adherence to legal and regulatory requirements
- Risk management policies and practices
- Financial information systems
- Testing of transactions' observance of limits
- Testing of compliance with regulatory requirements
- Special investigations

This just goes to show how critical the role of the internal auditor is. In addition, before auditors undertake any audit engagement it is important that they have a general understanding of the environment being audited, as well the technologies and systems being used in the organisation.

3.3.2 External auditors

The role of external auditors is to evaluate the reasonableness of financial statements, thus determining whether the financial statements properly reflect the performance of the business (Carrol 2006).

External auditors are usually tasked with performing the following functions (Chorafas 2008):

- Evaluate the work of internal auditors.

- Examine the organisation's accounting principles and its compliance with them.
- Analyse financial reports and disclosures.
- Test the assets, liabilities, revenues and expenses.
- Pay particular attention to high-risk areas.
- Appraise the performance of internal controls and their adequacy under stress conditions.

As can be noted, external auditors must, among other things, assess the work done by internal auditors. Then, depending on the outcomes of the evaluation of internal audit work, external auditors can perform further tests to satisfy themselves. To perform such tests, external auditors must possess vast skills related to consulting, performance analysis, operational review and information technology.

Nowadays, information systems are so pervasive and fundamental to a company's performance and, as such, evaluation of IT risks and controls, that they are crucial to company performance (Gonzales et al. 2004). This means that auditors must place reliance on the underlying systems that store, transport and process the transactions, as, if the controls on these systems are weak, auditors may lose confidence in the integrity of the information being processed and produced by those systems.

3.3.3 Auditing bodies and standards

The work of auditors is governed by various bodies that lay down rules and regulations that their members must abide by. At the international level, auditors and accountants are subjected to regulations established by the International Auditing and Assurance Standards Board, which falls under the International Federation of Accountants (IFAC 2011). In South Africa, auditors are regulated by the Independent Regulatory Body for Auditors (IRBA) (SA Government 2005). Further, ICT security auditors and information systems auditors are regulated by a body called the Information Systems Audit and Control Association (ISACA) (ISACA 2008b). Internal auditors, on the other hand, must adhere to the rules and regulations set out by the Institute of Internal Auditors (IIA) (IIA 2010). In addition, the

general standards that govern the audit profession are the General Accepted Auditing Standards (GAAS) (GAAS 2010).

There are other bodies and standards, but the scope of this study will focus only on the ones mentioned above. These will now be briefly discussed in the following sections.

3.3.3.1 International Auditing and Assurance Standards Board (IAASB)

The IAASB is an independent standard-setting body that serves the public interest by setting high-quality international standards for auditing, quality control, review and other assurance and related services, and by facilitating the convergence of international and national standards (IFAC 2011). In doing so, the IAASB seeks to enhance the quality and uniformity of practice throughout the world and strengthen public confidence in the global auditing and assurance profession (IFAC 2011).

3.3.3.2 Independent Regulatory Body for Auditors (IRBA)

The IRBA was established by the Auditing Profession Act of 2005 (SA Government 2005). The objective of the IRBA is to protect the financial interests of the South African public and international investors in South Africa through the effective and appropriate regulation of audits conducted by registered auditors, in accordance with internationally recognised standards and processes (IRBA 2011).

The statutory Committee for Auditor Ethics assists the Board in determining what constitutes improper conduct by registered auditors by developing rules and guidelines for professional ethics, including a Code of Professional Conduct for Registered Auditors and Rules Regarding Improper Conduct (IRBA 2011).

3.3.3.3 Information Systems Audit and Control Association (ISACA)

The ISACA is the body that sets standards and guidelines applicable to information systems auditors. Some of the standards set by ISACA include the following (ISACA 2008a):

- *Audit charter.* The purpose of an audit charter is to document the purpose, responsibility, authority and accountability of information systems (IS) auditors
- *Independence.* The auditor must be *professionally* and *organisationally* independent.
- *Professional competence.* Auditors must be professionally competent and have the skills required to run an audit.

There are many other standards defined by ISACA and to which the IS auditor must conform; failure to do so may lead to disciplinary action and possibly having membership suspended or revoked by the body.

3.3.3.4 The Institute of Internal Auditors (IIA)

The Institute of Internal Auditors serves the interests of internal auditors throughout the world (IIA 2010). Most of the standards defined by this institute are similar to those defined by ISACA. The purpose of the IIA standards is the following (IIA 2010):

- Delineate basic principles that represent the practice of internal auditing.
- Provide a framework for performing and promoting a broad range of value-added internal auditing.
- Establish the basis for the evaluation of internal audit performance.
- Foster improved organisational processes and operations.

In total, the body has about 17 standards statements which include:

- Purpose, authority and responsibility
- Independence and objectivity
- Proficiency and due professional care
- Quality assurance and improvement programme

3.3.3.5 General Accepted Auditing Standards (GAAS)

Auditors must adhere to the principles of the Generally Accepted Auditing Standards (GAAS) (GAAS 2010). The GAAS groups its rules into three areas:

- General standards
- Standards of field work
- Standards of reporting

General standards require that the audit be performed by persons with adequate technical training and proficiency, characterised by an independent mental attitude and being capable of exercising due professional care in audits. This includes overall performance, the discovery process, and preparation of the audit report (Chorafas 2008).

Standards of field work call for the audit to be adequately planned, supervision of auditors to be properly exercised, and a proper study and evaluation of existing internal controls to be made to determine the audit scope and the procedures to be performed during field work. Further, sufficient evidence must be obtained to formulate an independent factual opinion regarding internal controls (Chorafas 2008).

GAAS standards of reporting focus on the matters confronting internal and external auditors, such as whether records and other related artefacts are presented in accordance with GAAS. The application of GAAS in audited accounting records, statements and reports must achieve the fundamental objective of accounting, which is to provide reliable financial information about the economic resources and obligations of the organisation (Chorafas 2008).

3.3.4 Key items and tools for auditors

Similar to information security professionals, auditors need to approach their projects in a structured way. The following are key items that auditors must be able to understand and use effectively (Gonzales et al. 2004):

- *Audit preparation* – includes identification of the skills and resources required as well as sources of information.
- *Audit objectives* – formal statements describing the purposes of the audit.
- *Data gathering* – involves determining and implementing the sample selection approach. It also involves the means through which the data will be collected.

- *Audit programme* – a plan for reviewing and testing controls on each subject area. The controls are tested using the data collected.
- *Audit tests* – these are designed to verify the functional accuracy, efficiency and control of the area being audited.
- *Use of audit tools* – tools such as computer-assisted audit techniques (CAATs) are used by auditors to automate the process of evaluating large amounts of data spanning different systems.
- *Conclusions* – these are the opinions auditors formulate on the basis of the documented evidence before them.
- *Findings* – these are formal statements that highlight the weaknesses identified in terms of the controls implemented or not implemented by the organisation.
- *Recommendations* – these are corrective measures that auditors propose for resolving any problems identified by the findings.
- *The audit report* – this is the final document presented to the client after the audit has been concluded.
- *Working papers* – these include the systematic documentation of evidence compiled by the auditor thereby allowing him/her to arrive at a conclusion.
- *Follow-up of audit recommendations* – these are follow-up reviews to evaluate the progress made by the organisation in addressing the audit findings.

3.3.5 Continuous auditing

Owing to the constant changes taking place in systems within organisations, and the amount of information that is produced by business processes and transactions, auditors are faced with the challenge of how best to pick up irregularities before a large amount of damage is done. This then means that auditors must identify and implement ways that will provide assurance on an ongoing basis. To achieve this, auditors must look for technologies that provide continuous auditing.

While there are benefits to be extracted from implementing continuous auditing, there are nevertheless challenges involved in implementing it. Organisations run different systems on different platforms, including legacy systems. Therefore, the information being processed is also stored in different formats. This setup then limits the ability of the continuous auditing

solutions because data from different systems and in different formats must be standardised first before being analysed and presented. This consequently becomes an expensive process and is time consuming (Flowerday, Blundell & Von Solms 2006).

3.4 Regulatory environment

As noted earlier, information security forms part of corporate governance. Hence, corporate governance requirements oblige the organisation to comply with all laws and regulations that the organisation is operating under. In line with international trends, South Africa is paying increased attention to information protection and privacy issues. The enforcement of such regulatory requirements is performed by regulatory officials, who should have authority and integrity, as well as the necessary resources (OECD 2004).

As part of corporate governance, information security also forms part of enterprise risk management. Regulatory officials influence enterprise risk management for many organisations, either through requirements to establish internal controls or through the examination of particular entities. Regulatory influence happens in two ways: firstly, officials establish rules that provide the impetus for management to ensure that risk management and control systems meet the minimum statutory and regulatory requirements; and, secondly, pursuant to the examination of a particular entity, they provide information used by the entity to apply enterprise risk management, and make recommendations and sometimes directives to management regarding needed improvements (COSO 2004b).

Today, law makers are recognising the importance of information and the risks that face it. To address risks, various laws have been enacted locally and internationally and they need to be complied with. The challenge, however, is that various laws across different countries are inconsistent and are often incompatible (Sundt 2006). This then presents a special challenge for multinational companies which operate in different countries and, thus, by extension, need to comply with the laws of those countries. A very small number of laws and regulations prescribe how compliance is to be achieved; consequently, the onus falls on organisations to ascertain how they are going to meet the requirements of the laws and regulations. Such organisations must implement a correct, effective and affordable mix of

controls that ensures that the business meets its objective while ensuring that compliance with the law can be demonstrated (Sundt 2006).

3.4.1 Types of regulation

There are two types of regulation, namely, mandatory and advisory (Sundt 2006). Mandatory laws and regulations are those that must be complied with at all costs without exception. Failure to comply with these may lead to criminal charges being laid against the directors and/or senior management of the organisation concerned. Advisory regulations, on the other hand, are those that exist but are not legally enforceable. They may, however, influence the laws and failure to comply with them may exacerbate problems in any legal challenge (Sundt 2006). Complying with advisory regulations can also provide a competitive advantage for an organisation. In South Africa, for instance, King III is a code that prescribes how corporate governance should be implemented, but the code is not legally enforceable.

There are cases where a national law is enforced outside its strict legal jurisdiction. This is referred to as extra-territoriality (Sundt 2006). For example, the requirements of the law may be that notification be made of any security breach affecting the information of citizens of a particular country by any company anywhere in the world (Sundt 2006).

3.4.2 Regulatory bodies

Regulatory bodies enforce legal or regulatory requirements and compliance in this regard is usually mandatory. These bodies exist in various forms and have different focus areas. When information security professionals implement controls in an organisation, they need to be aware of the laws they must comply with and that regulatory bodies can at any time come and inspect the status of the implemented information security controls. Ideally, information security professionals should include legal counsel in decisions regarding information security and privacy and the formulation of policies around such matters (Fitzgerald, Krause 2008).

In the same vein, auditors must take into account existing laws affecting the organisation they are performing audits for. This then requires a mutual understanding among the three role players with regard to information security requirements.

South Africa, through its various laws and regulations, has seen the establishment of a number of regulatory bodies, as well as the existence of regulatory officials. The regulatory bodies that have an impact on the role players forming part of this study are discussed in the following sections.

3.4.2.1 COMSEC

One of the major players in the protection of information within the organs of state is COMSEC. COMSEC was established as the institutional authority to, among other things (Padayachie 2008)

- identify and protect the critical infrastructure
- protect and secure critical electronic communications of the organs of state against unauthorised access or technical, electronic or any other related threats

On an annual basis, COMSEC officials send questionnaires with a list of security questions to the various organs of state. The purpose of these questionnaires is to identify the security controls that are implemented within the organisation. Based on the answers COMSEC receives to the questionnaires, it may decide to visit a particular state organ to obtain more evidence.

3.4.2.2 Cyber inspectors

The ECT Act prescribes the appointment of cyber inspectors by the Department of Communications (DOC). These cyber inspectors may monitor internet websites in the public domain and investigate whether cryptography and authentication service providers comply with the relevant provisions of the Act. Inspectors have the powers of search and seizure subject to obtaining a warrant. They can also assist the police or other investigative bodies on request (Michalson, Hughes 2005).

3.4.2.3 National Cyber Security Advisory Council

In February 2010, the DOC released a draft cyber security policy document to the public for comment. The policy provides for the establishment of a National Cyber Security Advisory Council (NCAC) to coordinate all cyber security initiatives at the strategic level (Department

Of Communications 2010). Among the tasks allocated to the NCAC is to assess the state of national cyber security, determine needs and advise on appropriate responses and priorities. The council must also provide oversight regarding the implementation of national cyber security initiatives and structures.

3.4.2.4 National Computer Security Incident Response Teams

The draft cyber security policy further provides for the establishment of a National Computer Security Incident Response Team (CSIRT), whose role will be to identify, analyse, contain, mitigate and report the outcome of threats to the relevant parties. This team will be established by the DOC in conjunction with relevant government departments, the private sector and civil society (Department Of Communications 2010).

3.4.3 Private regulatory bodies

As discussed in chapter 2, through public–private partnerships there are other bodies that play a role in one form or another in the information security regulatory environment. These bodies, which are listed below, were discussed in chapter 2 because of the role they play in IT and financial matters:

- The South African Fraud Prevention Service (SAFPS), whose role is to assist in the protection against impersonation and identify theft.
- South African Banking Risk Information Centre (SABRIC), which provides intelligence support to banks against crime including e-crime.
- Business Against Crime South Africa (BAC), which focuses on commercial crimes including those committed using IT systems.

3.5 How does each role player contribute in the various stages of information security implementation?

(Dagada, Eloff & Venter 2009) have come up with a model based on the diagram below, which is meant to ensure that organisations meet the legal requirements when formulating

their information security strategies and implementing the same. The diagram consists of blocks 1 to 8; the actions that occur within each block will be discussed next.

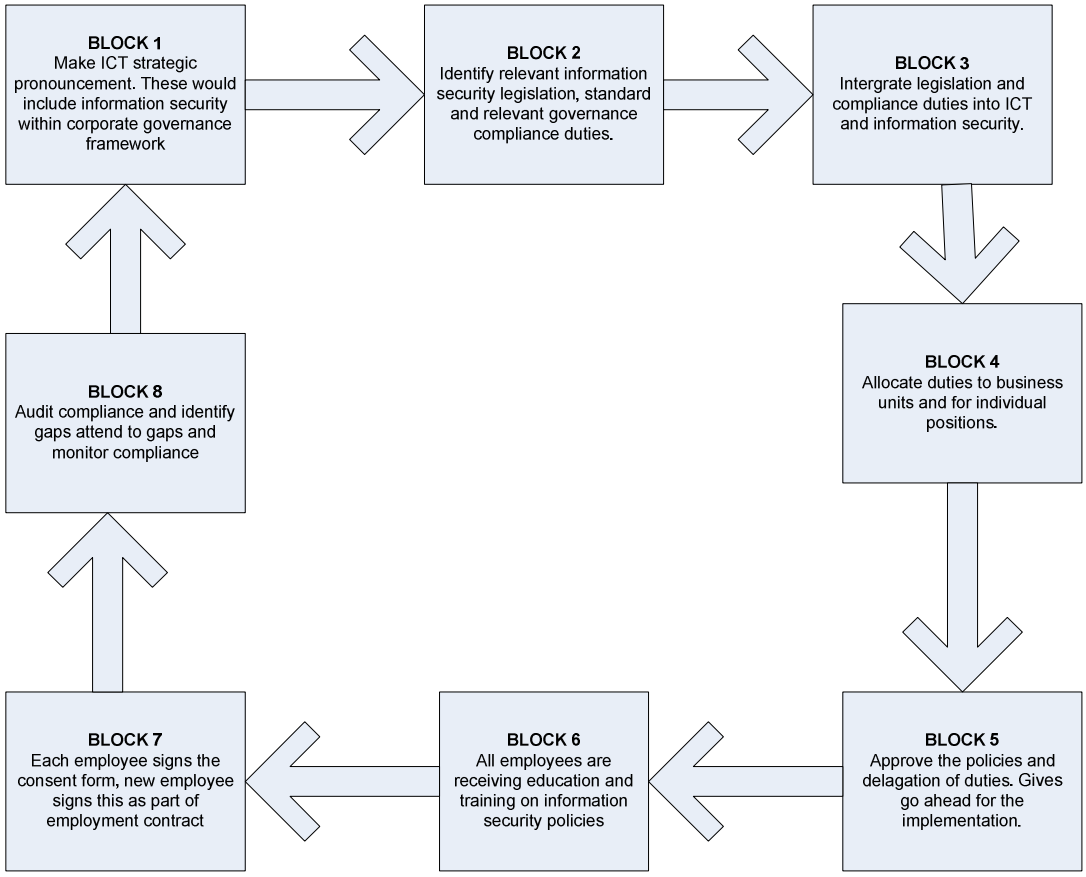


Figure 3.2 Model for ensuring information security complies with regulatory requirements (Dagada et al. 2009)

Block 1: First and foremost, an ICT strategic pronouncement should be made. This is made by senior management at the organisation's corporate level. These ICT strategies have implications for the information security requirements.

Block 2: The relevant legislation, codes and standards that must be complied with must be identified. This affects information security in particular since all information security initiatives must be in line with legislation and compliance requirements, as these are usually mandatory.

Block 3: Once the compliance and regulatory requirements have been identified, they should be integrated into the ICT security plan. The purpose of the security plan is to ensure

that the organisation meets its objectives while at the same time complying with all applicable compliance and legislation requirements.

Block 4–7: These blocks relate to the various stages through which policies progress, including the allocation of duties to particular units and the approval process, up to the point where each employee signs an acknowledgement of the approved policies. Importantly, user awareness should be integrated during these stages so that users will know what is expected of them and what the consequences of non-compliance are.

Block 8: This is where the regulatory officials and the ICT auditors play a critical role in verifying the compliance of the organisation in terms of the policies and regulatory requirements. At this stage, information security professionals must monitor controls regularly and implement corrective measures in case of non-compliance. They must also use the feedback from ICT auditors and regulatory officials to improve the controls. This may require a review of the security plan with a view to updating it where necessary.

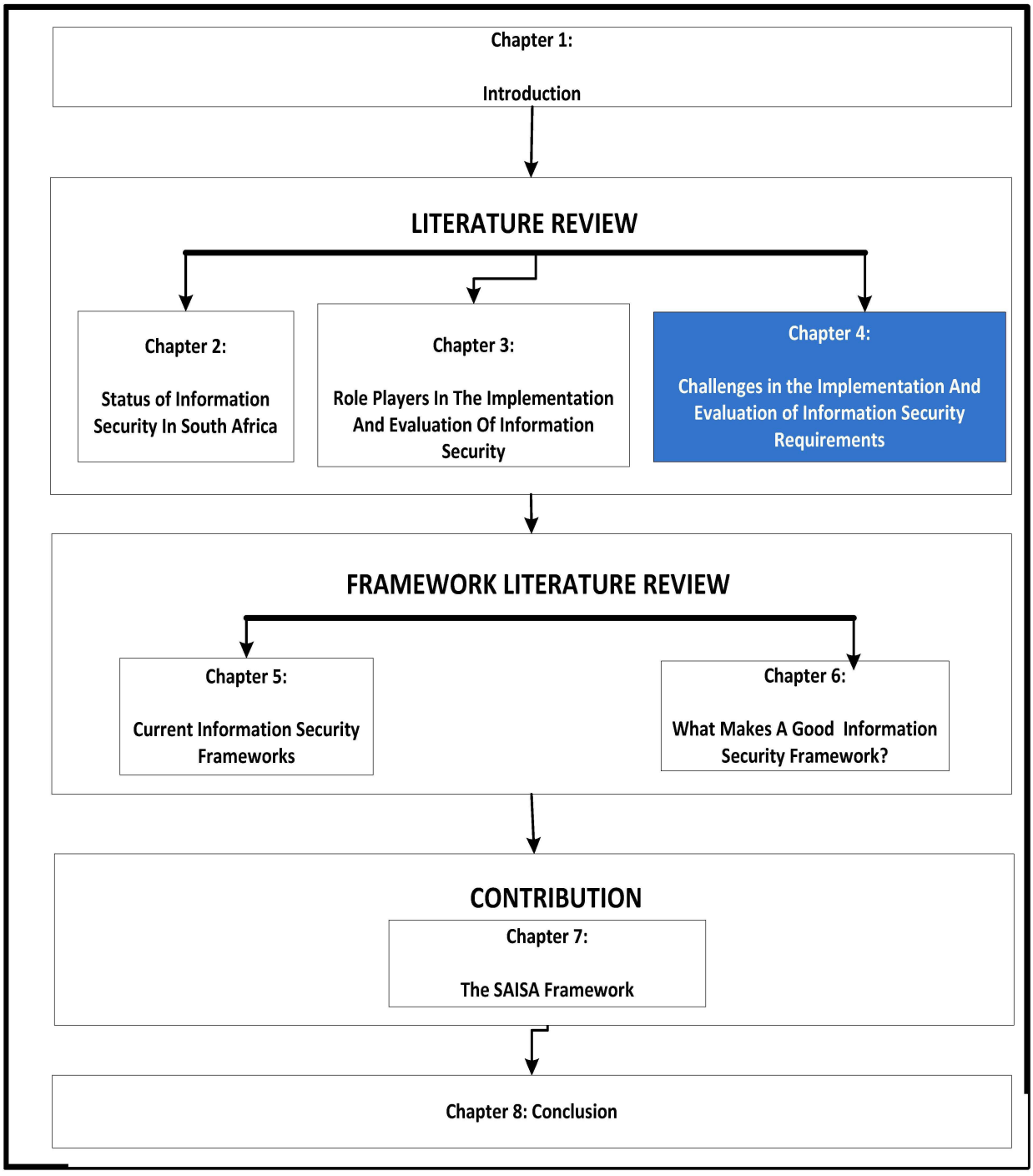
3.6 Conclusion

The discussion in this chapter has focused on the three role players involved in the implementation and evaluation of information security controls within an organisation. The three key role players were identified as information security professionals, ICT security auditors and regulatory officials. It was noted that since information security forms part of corporate governance, the same principles that are used to implement corporate governance must be used for information security. The coexistence of information security professionals, ICT security auditors and regulatory officials ensures that there are checks and balances which form the cornerstone of corporate governance.

The roles of the three role players were discussed in detail, as well as the various approaches and methodologies each role player can use in executing their duties. The next chapter will examine the challenges that exist in the implementation and evaluation of information security requirements.

Chapter 4

Challenges in the Implementation and Evaluation of Information Security Requirements


Chapter 1:
Introduction
LITERATURE REVIEW
Chapter 2:
Status of Information Security In South Africa
Chapter 3:
Role Players In The Implementation And Evaluation Of Information Security
Chapter 4:
Challenges in the Implementation And Evaluation of Information Security Requirements
FRAMEWORK LITERATURE REVIEW
Chapter 5:
Current Information Security Frameworks
Chapter 6:
What Makes A Good Information Security Framework?
CONTRIBUTION
Chapter 7:
The SAISA Framework
Chapter 8: Conclusion

4.1 Introduction

In the previous chapter, the focus was on the three role players (information security professionals, ICT security auditors and regulatory officials) that play a crucial role in the implementation and evaluation of information security controls. The discussion focused on their roles and responsibilities, as well as the standards that they adhere to. Accordingly, interaction among the role players is crucial in ensuring that they are aligned when initiatives are undertaken to implement and evaluate information security controls.

The role players must understand and interpret information security requirements consistently in order to avoid any unnecessary misunderstanding and conflict that may arise owing to misalignments regarding the implementation and evaluation of information security controls. Such conflict could lead to delays in projects, and could also affect security, as parties may be pulling against each other instead of working together (National Computing Centre 2005). In addition, wastage of scarce resources, such as time and money, could occur since a lot of energy may be expended debating issues rather than putting the actual controls required to protect information into place (Tucci 2009).

This chapter looks at challenges affecting the implementation and evaluation of information security controls. It discusses how the interpretation challenges among the role players lead to difficulties in the implementation of information security controls. It also covers factors such as money and skills shortages, information security trade-offs and communication barriers.

4.2 Business information security

The implementation of information security controls cannot happen in isolation from the other activities taking place in an organisation, as information security must be in line with the organisation's goals (ISO/IEC 27002 2007). To this end, the implementation of security controls in an organisation must not hamper the day-to-day business operations.

Role players must acknowledge and appreciate the resources involved in information security; these resources include people, process and technology (IT Governance Institute

2007a). The interactions among the role players have an influence on how information security is implemented and evaluated in an organisation (Hermason, Hill & Ivancevich 2000). This interaction is influenced by culture, human factors and support, architecture and governance, as indicated in figure 4.1 below (ISACA 2009a). Information security professionals, ICT security auditors and regulatory officials must understand these complex factors as they are the ones who implement and evaluate information security controls.

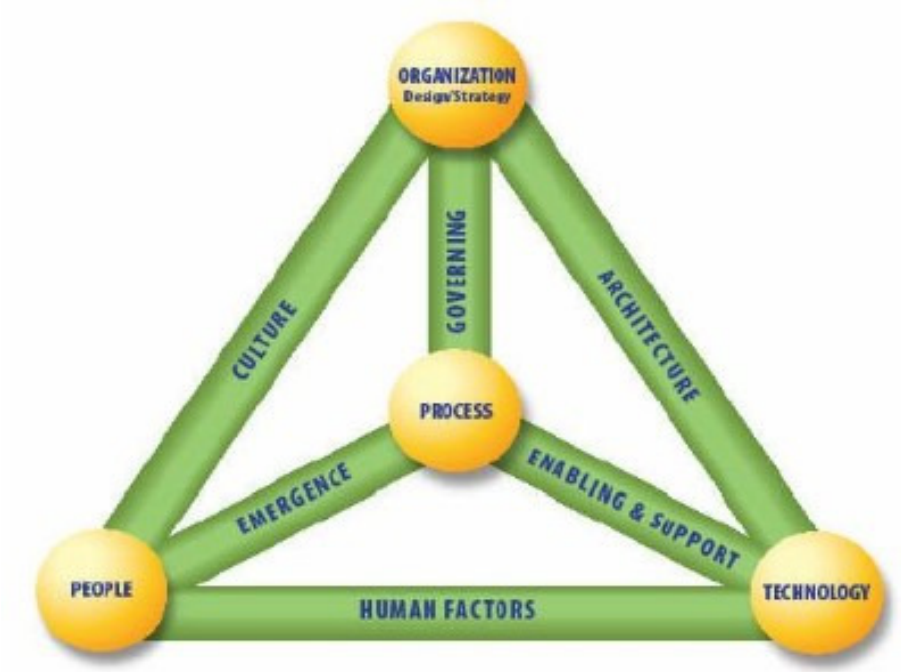


Figure 4.1 The Business Model for Information Security (ISACA 2009)

There is a general consensus among industry players that information security is not just a technology issue but also a business issue, which needs to be addressed at the highest levels of the organisation (IT Governance Institute 2006). In implementing an information security programme, the organisation is addressing business risk in ways that ensure that the business functions and strives. Aligning an information security programme to business requirements is a key element in putting in place solutions that address business risks (Onsett International Corporation 2001). Effective security management not only requires the selection of appropriate technology, but also organisational support, competent people and efficient processes (ISACA 2009a).

4.3 Information security requirements

Information security requirements come in different forms and change over time as the organisation evolves. Furthermore, as systems evolve as a result of changes in their requirements and the environment in which they operate, security requirements need to be re-validated, or changed, to ensure an appropriate level of asset protection (ThesisTown 2009). Examples of information security requirements include the following (Fitzgerald, Krause 2008, Gerber, Von Solms 2001):

- Maintain confidentiality, integrity and availability of services.
- Act competitively while being secure and meeting privacy and regulatory requirements.

For any organisation to embark on implementing any information security initiative, it is critical that the information security requirements for the organisation be clearly articulated and understood as early as possible.

4.3.1 Sources of information security requirements

To properly define information security requirements, there must be a source of information that provides a basis for the decisions being made on information security goals. There are three sources of information security requirements (ISO/IEC 27002 2007, Fitzgerald, Krause 2008):

- Identification of information security risks that are unique to the organisation
- Legal, statutory, regulatory and contractual obligations
- Uniqueness of the organisation

4.3.1.1 Identification of information security risks that are unique to the organisation

Risk comprises three main components: the asset, a threat and the vulnerability of the asset to the threat (Gerber, Von Solms 2005). An asset is anything that has value to the organisation (ISO/IEC 13335 2004), while vulnerability is a weakness in the security system

that might be exploited to cause loss of or harm to the assets (Gerber, Von Solms 2005). On the other hand, a threat is the source or the circumstance that has the potential to cause loss or harm (Gerber, Von Solms 2005). Information is an asset of value to an organisation and, as a result, needs to be properly protected in order to ensure business continuity, minimise business damage, maximise return on investment (ROI) and exploit business opportunities (OregonGov 2009).

During the risk assessment process, three components must be taken into account: the value of the information asset, the likelihood of a threat being realised and the vulnerability between two (Jackson, Hruska 1992). As discussed in the previous chapter, various tools and frameworks (both qualitative and quantitative) can be used to identify the risks unique to the organisation.

The outcomes of the risk assessment exercise are the recommended information security controls that must be implemented based on the calculated risk values (Gerber, Von Solms 2001). Each adverse event identified during the risk analysis exercise must have an impact associated with it, as well its likelihood of occurring. Each risk identified must be categorised in any of the four categories as illustrated in figure 4.2 below:

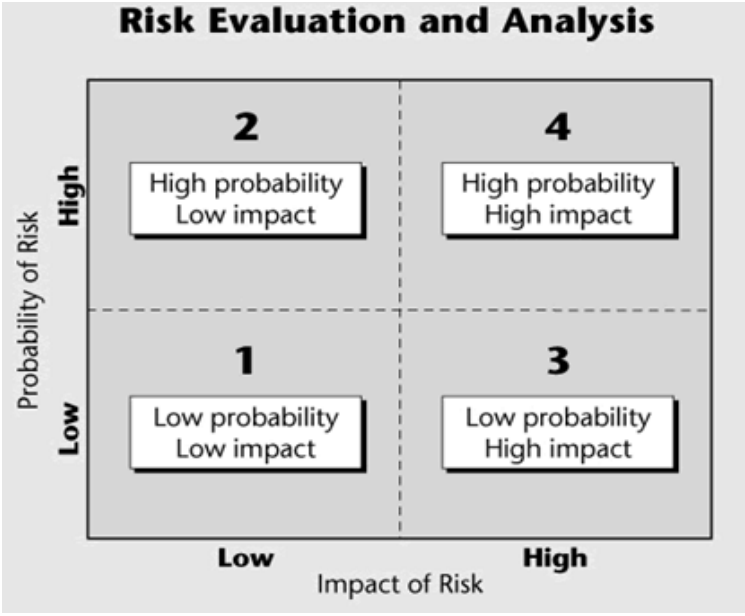


Figure 4.2 Risk evaluation and analysis (Qayoumi & Woody 2005)

Based on figure 4.2 above, the risks that fall into category 4 (those with high probability & high impact) must receive immediate attention. These are the risks that, if realised, would have maximum impact. They also have the highest probability of occurring. Typically, the risks in category 4 would be placed on top of a priority list for addressing information security risks.

The risks falling into category 1 (low probability & low impact) would be at the bottom of a list of the risks that need to be attended to. In fact, the organisation may find cost-saving opportunities by decreasing the degree of control or by assuming more risk (ISACA 2009b). It is important for information security professionals to understand which risks fall under the different categories in order to have a better understanding of the areas that should receive most of their efforts and resources.

ICT security auditors should also understand which areas to focus on when performing their reviews so that they do not focus their efforts on areas that are of least importance and which information security professionals are not paying immediate attention to. In this regard, risk management helps ICT auditors in the following ways (ISACA 2008a):

- It assists auditor in identifying the risks and threats to an ICT environment and the systems that would need to be addressed by management and system-specific controls. Identifying the different levels of risk may assist the auditor in making better selections of areas to examine (with bias towards high-risk areas).
- It helps auditors in their evaluation of controls in audit planning.
- It assists auditors in determining audit objectives.
- It supports risk-based audit decision making.

Risk management is also important for regulatory officials. As noted earlier, regulatory officials influence the risk management of many entities, either with requirements to establish internal controls or through examinations of particular entities (COSO 2004b).

The first step in the risk assessment process is to collect information on the system (asset). This happens by looking at the characteristics of the asset in question. The next step requires the system security to be defined. Inputs to this step are the identification of the protection needs of the systems, as well as the criticality/sensibility of these needs. In the step that

follows, system threats and system vulnerability analyses are carried out. Once the system vulnerability analysis is complete, the likelihood of the threat being realised and other information like the severity/criticality of the impact are defined. These can be ranked according to 'high', 'medium' and 'low', which feeds into the rating using the table illustrated in figure 4.2. The final step is to produce a risk assessment report. This report contains findings and recommendations regarding any additional security controls. Information security professionals use this report to start the process of implementing security controls in an environment.

4.3.1.2 Legal, statutory, regulatory and contractual obligations

Standards for compliance, review, monitoring and oversight functions must be incorporated into the overall security infrastructure to ensure that all legal requirements are met (IIA 2010). Every organisation, regardless of its size or the industry in which it operates, needs to comply with a number of governmental and external requirements related to computer system practices and controls, and to the manner in which computers, programs and data are stored and used (ISACA 2008a). Furthermore, business regulations can impact on the way data is processed, transmitted or stored. Any organisation should establish accurately which legal, regulatory or statutory requirements they are subject to in terms of their own business practices, their business partners and government (Gerber, Von Solms 2001).

In South Africa, as discussed in chapter 2, many laws and regulations exist that have an effect on how information security is implemented. These include the ECT Act, COMSEC, RICA and King III. Accordingly, companies must find a balance between meeting their security goals while ensuring that the compliance with regulatory requirements is met. This means that, as information security requirements are being formulated, certain legal, statutory, regulatory and contractual obligations must be taken into account.

Organisations using the services of counsel and legal advisors must understand and appreciate the legal requirements as they put into effect their information security programmes. The difficulty facing organisations is that few laws and regulations specify how compliance is to be achieved (Sundt 2006). It is then left up to organisations to decide on how they will go about achieving compliance. The result of this is that, in many cases, the

way in which legal and regulatory requirements are met depends more on people and procedures than on technical controls (Sundt 2006).

Organisations that fail to address legal and regulatory issues will find themselves at a competitive disadvantage and may fall victim to ever more technologically sophisticated criminals. Listed companies will find their share value increasingly being tied to governance (good and bad), as the market becomes more aware of its relevance (IT Governance Institute 2006).

4.3.1.3 Uniqueness of the organisation

Every organisation has unique vulnerabilities, imperatives and options requiring an individual security approach (International Chamber Of Commerce 2003). No two organisations are alike, therefore neither are their information security requirements. The uniqueness of an organisation relates to the principles, objectives, procedures and requirements it has adopted to process information in support of its business operations and processes (Anderson 2002). During the requirements analysis stage, the required levels of confidentiality, integrity and availability should be determined for the organisation. Once the organisation has decided how much security it requires, suitable controls can be identified that satisfy those requirements (Butler 2006).

The organisation's unique risks can be elicited from its strategy, enterprise architecture and applicable codes and the industry in which the organisation is operating. In terms of the industry, companies are often encouraged to meet the security standards of their particular industry or sector (International Chamber Of Commerce 2003). This not only saves the company the associated penalties and reputational risks, but it also gives them a competitive edge over competitors (Hermason, Hill & Ivancevich 2000).

4.4 Factors affecting the implementation of information security controls

The identification of legislation affecting information security and the development of information security strategies and policies, although important, are only the first steps in

the organisation's information security programme. The next important step is the implementation of controls based on those documents. This is important because, for example, the policy/law may look good on paper, but if it cannot be enforced then its purpose is defeated. The enforcement and implementation of information security controls require a number of critical elements: money, time, skill (Hoffman 2007) and coordination. Information can also be looked at from different viewpoints: attackers versus defenders, security versus usability, or security as an afterthought (Owens 2009). These will now be looked at in detail to determine how they affect the implementation and enforcement of information security controls.

4.4.1 Money

The protection of information assets creates new and unwanted costs, where costs are defined as expenditure on resources that detect and prevent security breaches (Anderson, Choobineh 2008).

Organisations, however, have limited financial resources which must be spent on other areas in addition to investments on information security controls (Business Software Alliance 2003, Courtney 1982).

To enforce information security controls, money is required to do the following (Anderson, Choobineh 2008, International Telecommunication Union 2008):

- Put preventative measures in place.
- Recruit and retain skilled people.
- Investigate any breaches that occur.

4.4.1.1 Putting preventive measures in place

Preventive measures include controls such as properly configured technologies (e.g. firewalls and intrusion detection/prevention systems), user awareness, ongoing support and maintenance of information security systems.

4.4.1.2 Recruiting and retaining skilled people

Information security is a complex subject that requires suitably trained people to implement security controls (ISACA 2009a, Trcek 2003, Von Solms, Von Solms 2004). Retaining such people is an expensive exercise, as there is always the risk that they will be poached by other companies, including international firms, as a result becoming more expensive to keep.

4.4.1.3 Investigating a breach

No matter how many preventive controls are in place, there can never be a 100% secure system and environment – there is always a residual risk. When a breach occurs, an investigation should follow into what actually happened and, based on the investigation results, further action can be taken.

During such investigations, evidence must be produced and preserved for law enforcement agencies. Investigations are costly and financial resources have to be made available to ensure they are successful. Firstly, skilled people are required to conduct investigations related to information security breaches. Secondly, sophisticated technologies must be deployed to help with such investigations. The rapid evolution of technology and information security breach techniques mean that law enforcement agencies must continuously upgrade technical equipment and software tools (Powner 2005). Such equipment and tools are expensive. Moreover, the logs produced by systems can be voluminous and may need a huge amount of memory storage.

4.4.2 Skills

Regulatory officials find that maintaining a current understanding of new criminal techniques and technologies can be difficult. For example, law enforcement agents may be rerequired to extract forensic data from IT devices that have only been on the market for a few months. They must also keep abreast of innovative criminal techniques and approaches. In addition, criminals are increasing their use of encryption techniques, making it difficult to read what is inside a communication (Powner 2005).

After an investigation has been completed, it should be taken to courts if it is a criminal matter. This means that judges, lawyers and prosecutors must have the skills required to assess information security related cases. In addition, they must have both law enforcement and technical skills, including knowledge of various IT hardware and software and forensic tools. According to (Powner 2005), state and law enforcement agencies do not have the resources needed to hire investigators with the technical knowledge required to address information security crimes.

4.4.3 Time

To implement and enforce the law requires time. Generally, laws affecting systems require system changes, reconfiguration or the introduction of new technologies. Besides the required changes to the systems, the people of the country must acclimatise themselves to new laws and abide by their provisions before they can fully understand them. The time required for this could range from months to years. While this is taking place, attackers are not biding their time, they are busy launching attacks.

4.4.4 Coordination

Coordination and cooperation between different agencies, including the public and the private sectors, are of paramount importance. The reporting of information security related breaches is often hampered by the fact that companies are reluctant to report security breaches of their systems. According to (Powner 2005), the reasons for this include the following:

- *Financial market impacts*. The stock and credit markets and bond rating firms react negatively to security breach announcements, which could raise the cost of capital to the affected organisation. Even firms that are privately held and are not active in public securities markets can be adversely affected if banks and other lenders judge them to be more risky than previously thought.

- *Reputation or confidence effects.* Negative publicity damages a reporting firm's reputation or brand, and could cause customers to lose confidence, giving commercial rivals a competitive advantage.

- *Litigation concerns.* If an organisation reports a security breach, investors, customers, and other stakeholders can use the courts to claim damages. If the organisation has been open in the past about previous incidents, plaintiffs may allege a pattern of negligence.

- *Signal to attackers.* A public announcement alerts hackers to the fact that an organisation's information security defences are weak and may inspire further attacks.

- *Inability to share information.* Some private-sector entities want to share information about an incident with law enforcement and other entities; however, once the information becomes part of an ongoing investigation, their ability to share information may be limited.

- *Job security.* IT personnel may fear for their jobs after an incident and seek to conceal the breach from senior management.

- *Lack of law enforcement action.* If there is a perception that law enforcement entities fail to investigate cases reported to them, it could become a disincentive for reporting breaches in the future.

- *The borderless nature of breaches.* The borderless nature of information security gives rise to its own unique challenges. It is usually very difficult to investigate and prosecute security breaches that cross national borders and to work with laws, legal procedures and law enforcement entities from multiple jurisdictions. Hackers can be physically located in one nation, direct their activities through computers at multiple nations, and store evidence of their activities on computers in yet another nation.

Furthermore, law enforcers from one country may be uncooperative with another country when investigations are being conducted and prosecutions sought.

4.4.5 Attackers vs defenders

Information security professionals are faced with many challenges as they try to protect the organisation's assets. On the other hand, attackers have plenty of advantages on their side and these include the following (Owens 2009):

- Attackers need to only 'know' one vulnerability, while defenders need to secure all entry points.
- Attackers have unlimited time, while defenders work within time and cost constraints.

4.4.6 Security vs usability

Users always prefer to use a system that is easy to operate. However, information security controls may have the opposite effect on ease of use, for example (Owens 2009):

- Overly or improperly secured systems can be difficult to use.
- Complex and strong passwords can be difficult to remember.
- Users prefer simple passwords.

Providing adequate protection to information systems requires striking a balance between the security and the usability or productivity of the systems. Trying to strike such a balance requires stakeholders to make strategic decisions to achieve the desired level of security while trading off competing requirements such as costs, performance and usability (Liu, Yu & Mylopoulos 2002).

4.4.7 Security as an afterthought

One of the major challenges facing information security professionals is that security is often treated as an afterthought, or as optional, rather than being an integral part of a system's hardware and software (Mouratidis, Giorgini & Manson 2005, Wilson 2008). As such,

security add-ons are often poorly integrated with the rest of the system and are seen as an impediment rather than an enabler (Tipton, Krause 2004). Even when security is an integral feature of a product, it may be poorly implemented (Wybourne, Austin & Palmer 2009). Adding security features after the system has been designed and implemented is usually very costly and often without any guarantee that the added security will work well to combat security threats.

It is, however, important to note that (Owens 2009)

- many developers and management think that security does not add any value and is negative to the user's experience
- addressing vulnerabilities just before or after a product is released is very expensive

4.5 Information security controls and trade-offs

Implementing security goals is not always a straightforward activity; it requires leadership and a sense of understanding of what needs to be delivered taking into account the budgetary and resource constraints. In this regard, information security professionals and management have to consider trade-offs and related issues when they scrutinise and make information security investment decisions (Dlamini, Eloff & Hone 2009). Information security goals are largely determined by understanding the following trade-offs (Qayoumi, Woody 2005):

- *Services offered versus security provided*. Each service offered to the users carries its own security risks. For some services the risk outweighs the benefit of the service, and information security professionals and business persons may choose to eliminate the service rather than secure it.

- *Ease of use versus security.* As highlighted above, the easiest system to use is a system with no security at all, for example not requiring any sort of authentication such as passwords or any other security controls. The addition of security controls such as the requirement for passwords makes it less convenient to use but more

secure. Requiring device-generated, one-time passwords makes the system even more difficult to use but even more secure.

- *Cost of security versus risk of loss*. There are many different costs associated with security: monetary, performance and ease of use. In addition, there are different types of risk: loss of privacy, loss of data and loss of service. Each type of cost must be weighed up against each type of loss. The security control being implemented must deliver some value to the business. As the organisations invest in information security initiatives, they have to assess the resultant business returns. Linking information security initiatives to financial investment may help organisations to evaluate cost/benefits and thus improve the effectiveness of management information security (Huang, Lee & Kao 2006).

  Determining the financial value of information assets has its own difficulties. The challenge is that information assets protected by information security controls are intangible capital, and their value is difficult to assess (Huang, Lee & Kao 2006). As organisational assets (information) continue to become more intangible, the requirements of due care in the protection of information assets will require greater attention and resources (IT Governance Institute 2006). Further, current models also tend to be static and simple while IT environments are continuously changing (IT Governance Institute 2006). This means that current models fail to provide insight on how the organisation changes or how the culture evolves and, as a result, what may or may not emerge.

4.6 Communication barriers

The language used by information security professionals and business managers sometimes differs. This is despite the fact that they are both pursing the same goal. Information security managers strive to ensure that their programmes help the enterprise meet its strategic and operational goals; however, this can be a difficult task, for instance when they (information security professionals) are speaking in terms of specific threats, risks, controls and technologies, while business managers are talking about cost, productivity and ROI (IT Governance Institute 2006).

The complexity of this cross-communication is compounded by the fact that security is often defined inconsistently throughout the business. For the financial manager, security may equate to minimising financial risk and loss, while to the sales manager it is ensuring that nothing interferes with sales efforts and achieving targets. Meanwhile, the legal department sees it as a function of regulatory compliance, while a board member regard it as protection from personal liability (IT Governance Institute 2006). Consequently, it is of the utmost importance that the various information security investments be measured and clarified for effectiveness if information security is to be implemented and managed properly.

4.7 Conclusion

This chapter identified some of the key challenges in the implementation and evaluation of information security controls. These challenges result from a combination of issues. Moreover, information security is a complex subject that must be integrated into business activities. Accordingly, information security programmes must be based on a proper plan that involves performing risk assessment exercises and understanding the sources of information security requirements. To perform these activities, the role players are expected to possess a variety of skills that allows them to link business requirements and information security activities.

Implementing information security requires the investment of resources such as money, time and human resources. These resources are limited and information security faces competition from other business operations that want a share of these resources. Identifying, recruiting and retaining skilled human resources in the area of information security is not an easy task.

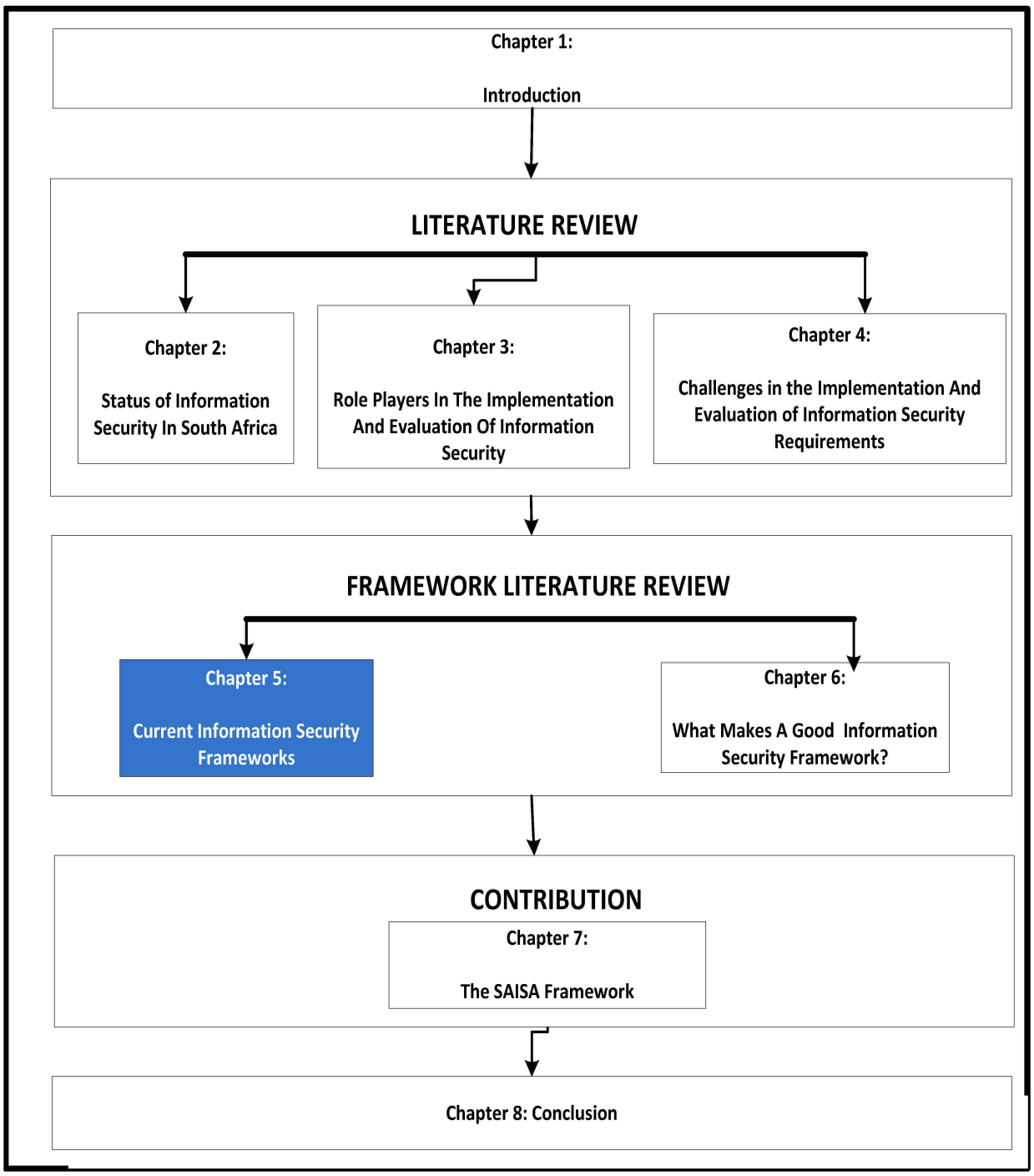
Reporting of security breaches does not happen often enough, thus the opportunity to share experiences on such breaches among different businesses and organisations is lost. Other matters affecting the implementation of information security include balancing security and usability, security being treated as an afterthought and communication barriers.

Frameworks and standards have been developed to address the challenges facing organisations regarding information security implementation and evaluation. The next

chapter will look at the main frameworks and standards that currently exist. Each framework being studied will be evaluated to determine its main purpose, its strengths and its weaknesses. This will help in the formulation of a framework that does not duplicate the existing frameworks but instead builds on them in developing a new and improved framework. Chapter 5 will also include some elements of the literature review as well the framework components.

Chapter 5

Current Information Security Frameworks


Chapter 1:
Introduction
LITERATURE REVIEW
Chapter 2:
Status of Information Security In South Africa
Chapter 3:
Role Players In The Implementation And Evaluation Of Information Security
Chapter 4:
Challenges in the Implementation And Evaluation of Information Security Requirements
FRAMEWORK LITERATURE REVIEW
Chapter 5:
Current Information Security Frameworks
Chapter 6:
What Makes A Good Information Security Framework?
CONTRIBUTION
Chapter 7:
The SAISA Framework
Chapter 8: Conclusion

5.1 Introduction

The previous chapter covered the challenges facing organisation with regard to implementation and evaluation of information controls. To resolve these challenges, organisations use information security frameworks to guide them on the controls they need to put in place in order to protect information assets in an organisation (Da Veiga, Eloff 2007). Currently, there are plenty of frameworks that influence information security. These include ISO/IEC 27002, and the standards of good practice for information security by the Information Security Forum (ISF), the Control Objectives for Information and Related Technology (COBIT) and the Information Technology Infrastructure Library (ITIL). Different frameworks are applicable to the different levels of an information security programme. The levels, illustrated in figure 5.1 below, are strategic, tactical and operational (technical) (Garigue, Stefaniu 2003, Von Solms, Von Solms 2006a).

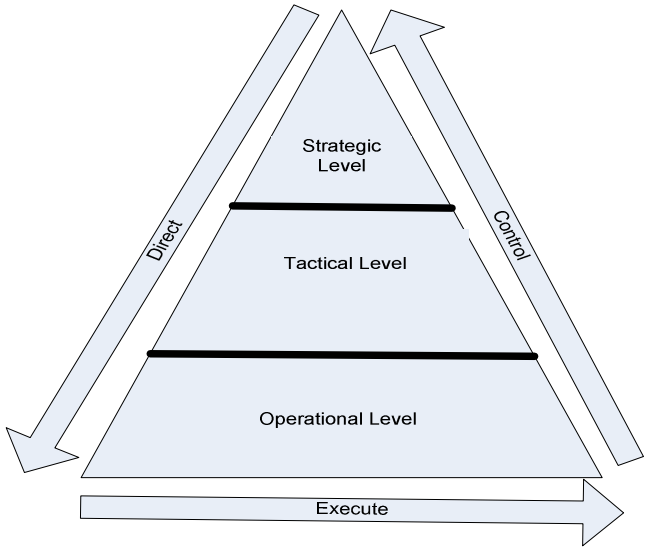


Figure 5.1 Security model (Von Solms & Von Solms 2006a)

This chapter focuses on the existing frameworks that influence information security and their importance. The discussion seeks to establish the objectives of each framework, including its strengths and weaknesses. This chapter will also determine whether each framework appeals to all or just some of the role players (information security professionals, ICT security auditors and regulatory officials). Understanding this will provide the necessary

input for formulating a new and comprehensive framework that will be used by all three role players to implement and evaluate information security controls.

5.2 The importance of information security frameworks

An organisation's objectives should be viewed in terms of four key dimensions, namely, strategic, operations, reporting and compliance (COSO 2004b). The strategic dimension relates to high-level goals, while the operations dimension relates to the effectiveness and efficiency of an organisation's operational processes. Further, the reporting dimension includes the capability of the organisation to report to internal and external stakeholders, while the compliance dimension is more concerned about the capability of the organisation to abide by the applicable laws and regulations and its need to do so (COSO 2004b).

With information security being a critical area in an organisation, it becomes important for it to be incorporated into the strategic, operational, reporting and compliance dimensions of the organisation's objectives. Following this approach ensures that information security becomes an integral part of the internal controls of the organisation. This approach further ensures that the expectations of the three role players are attended to and accommodated in the organisation's goals and objectives. Accordingly, the interests of information security professionals are focused on strategic and operational dimensions; the interests of auditors are particularly focused on reporting dimensions; while the focus of regulatory officials is inclined towards compliance.

To ensure that the organisation's information security needs are met and that the regulatory requirements are incorporated in information security related activities, the use of best practice frameworks should be strongly considered, as they help guide organisations in establishing effective governance (Lessing 2008). Frameworks also play a huge role in ensuring that IT resources are aligned with the organisation's objectives, and that the organisations information meet quality, fiduciary and security requirements (IT Governance Institute 2008a).

The adoption of a framework contributes to the quick implementation of good practices and avoids lengthy delays in creating and agreeing on new approaches that simply reinvent the

wheel (IT Governance Institute 2008a). This then contributes positively to ensuring that organisations approach information security in a structured manner. Having a framework goes a long way in embedding information security in the four dimensions of the organisation's objectives.

5.3 Types of framework

Depending on the objectives involved, frameworks have varying appeal to different role players. For example, one framework may appeal to information security professionals but not necessarily to ICT security auditors or vice versa. This may be as a consequence of the fact that each framework is developed to meet a particular need and therefore has a particular focus. Therefore, frameworks vary in terms of objectives, steps, structure and level of application (Saleh, Alfantookh 2011).

There are four types of framework that have an impact on information security. Firstly, there are generic frameworks that are high level in nature (e.g. COBIT). These frameworks focus on 'what' must be done rather than on 'how' it must be done (Furner, Cheney 2008). They are strong in providing the high-level integration required to ensure the cohesion of various components of information security programmes. Such frameworks are generally strategic in nature.

The second type of framework comprises those that are more detailed and technical in nature (e.g. ITIL). These frameworks provide the guidelines on 'how' things should be done (Furner, Cheney 2008) and are not as abstract as the high-level frameworks. These detailed frameworks are more oriented to the operational aspects of information security.

The third type of framework consists of those that are compliance focused (e.g. Basel II) (Furner, Cheney 2008). These are established by regulators to help organisations comply with certain regulations.

The final type of framework discussed here comprises those that consist of high-level guidelines (Furner, Cheney 2008). These are broad in nature and may focus on an area that spans many disciplines, for example the Committee of Sponsoring Organizations (COSO), which focuses on risk management in general. COSO can be used by different disciplines,

including IT, finance and law. Such frameworks are not necessarily IT focused but have an impact on IT. They can be used by information security professionals to, for instance, develop their own frameworks based on the principles of the high-level guideline frameworks. ICT security auditors can adopt such frameworks to assist in formulating their audit programmes.

5.4 Current and common frameworks and standards

There are many frameworks related to information security that can be used by organisations in conjunction with standards to implement and evaluate security controls. A **standard** is rigid and specifies one way of doing things (best practices) and these must be followed exactly as specified (Olivia 2011, Nair 2009). A **framework**, on the other hand, is flexible, and is not defined by a step-by-step process. Frameworks define the boundaries and the system, but not the method itself (Olivia 2011, Nair 2009).

For the purposes of this study, examples of both standards and frameworks will be looked at. However, the outcome of the research will be a framework, not a standard. The new framework will be flexible and adaptable to the various scenarios, and based on the needs and circumstances experienced by the role players.

This study will not look at all standards and frameworks related to or having an impact on information security, but will instead focus on the commonly used standards and frameworks. The frameworks examined in this chapter are spread across various types as discussed on section 5.3 above (i.e. the “what”, “how”, compliance and high level guideline frameworks). The frameworks chosen also touch on different aspects of information security, for example governance, risk management and compliance.

The common standards and frameworks that can be used in the implementation of information security include COBIT, ISO/IEC 27002, COSO, PCI-DSS, BASEL, ITIL, and the Standard of Good Practice for Information Security (FIC 2004, Spremic 2011, Ula, Ismail & Sidek 2011)(FIC 2004).

In chapter 3 it was highlighted that risk management is one of the key components of information security. To this end, frameworks with a particular focus on risk management

will also be examined here. Common risk management frameworks that will be discussed in the following paragraphs include OCTAVE, CRAM, ISRAM and CORA (Vorster, Labuschagne 2005).

As architecture has an impact on information security (Eloff, Eloff 2005), some of the frameworks subsequently examined in this chapter, that is, SABSA and the Zachman Framework, are architecture oriented.

The various frameworks and standards will be briefly discussed in the next few paragraphs.

5.4.1 ISO/IEC 27002

ISO/IEC 27002 is a comprehensive set of controls comprising best practices in information security (Trinckes 2009). This framework focuses on business, management, human resources and technology aspects to ensure that an efficient information security management programme is created (Trinckes 2009). The ISO 27002 framework defines 133 security controls under the following 11 focus areas (ISO/IEC 27002 2007):

- Security policy
- Organisational security
- Asset classification and control
- Personnel security
- Physical and environmental security
- Communications and operations management
- Access control
- Systems development and maintenance
- Incident response
- Business continuity
- Compliance

ISO/IEC 27002 is a useful tool for information security professionals for driving and implementing their information security programmes.

5.4.2 The Standard of Good Practice for Information Security by Information Security Forum

The Information Security Forum (ISF) produces the Standard of Good Practice for Information Security, which seeks to address information security from a business perspective (ISF 2007). The ISF is a membership-based organisation and the standard is targeted at members of the organisation, although non-members can obtain it for a fee.

The standard is aligned with other security-related standards such as ISO/IEC 27002 and Cobit (ISF 2007). The development of the standard is based on three main activities: an extensive work programme involving the expertise of a full-time ISF management team, analysis; and the integration of information security-related standards (e.g. ISO 27002) as well as the involvement of ISF members (ISF 2007).

The standard is aimed at major national and international organisations. The standard's target audience is information security managers, business managers, IT managers, IT audit managers and outsource providers (ISF 2007). It covers the following aspects of information security: security management (enterprise-wide), critical business applications, computer installations, networks, systems development and end user environment (ISF 2007).

5.4.3 The Payment Card Industry (PCI) Data Security Standard (DSS)

The PCI DSS can be defined as the following:

> A multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. This comprehensive standard is intended to help organisations proactively protect customer account data (PCI DSS 2011).

The PCI DSS is governed by the PCI Security Standards Council. This standard is applied to any entity that processes, stores or transmit credit card information (Apani 2006). The three main groups affected by the standard are the following (Apani 2006):

- *Merchants*. Retail stores that accept credit cards as payment.
- *Merchant banks or acquirers.* Process transactions on behalf of merchants.
- *Service providers*. Process, store, or transmit cardholder data on behalf of Visa members, merchants, or other service providers.

The standard has six focus areas (PCI DSS 2011):

- Build and maintain a secure network.
- Protect cardholder data.
- Maintain a vulnerability management programme.
- Implement strong access control measures.
- Regularly monitor and test networks.
- Maintain an information security policy.

5.4.4 Control Objectives for Information and Related Technology (COBIT)

Control Objectives for Information and related Technology (COBIT®) is a set of good practices that spans a domain and process framework (IT Governance Institute 2007a). It seeks to bring together business risks, control needs and technical issues by providing good practices to structure and manage activities (Trcek 2003). COBIT is high level and is focused on **what** is required to ensure the adequate management and control of IT.

COBIT is divided into four high-level domains, namely (IT Governance Institute 2007a):

- *Plan and organise (PO)* – provides direction to solution delivery (AI) and service delivery (DS).
- *Acquire and implement (AI)* – provides the solutions and passes them to be turned into services.
- *Deliver and support (DS)* – receives the solutions and makes them usable for end users.
- *Monitor and evaluate (ME)* – monitors all processes to ensure that the direction provided is followed.

COBIT appeals to a broad range of users in particular executive management, business management, IT management and auditors (IT Governance Institute 2007a).

5.4.5 Information Technology Infrastructure Library (ITIL)

The ITIL is a comprehensive best practice framework that provides guidelines on a wide range of aspects of service management (Rudd 2004). The framework covers the complete spectrum of people, processes, products and use of partners. The primary focus of the ITIL framework is service management. By adopting the ITIL, the organisation ensures that it improves the focus on information security as a business and a service. Through this,

information security moves from being perceived as a cost centre or hindrance to business functions, to a critical service that must be aligned to the overall business strategy (Weil 2010).

The modules that form part of the ITIL framework are the following: Service Delivery, Service Support, ICT Infrastructure Management, Planning to Implement Service Management, Application Management, the Business Perspective and Security Management (Rudd 2004).

5.4.6 Policy Framework for Interpreting Risk in e-Business Security (PFIRES)

The PFIRES was initially developed for e-commerce activities. It now also involves the handling of security policy for all types of organisation engaged in computing and internet operations (Rees, Bandyopadhyay & Spafford 2003). It offers a possible starting point for understanding the impact of security policy on an organisation, and is intended to guide organisations in developing, implementing and maintaining their security policy (Rees, Bandyopadhyay & Spafford 2003).

The PFIRES phases consist of assess, plan, deliver and operate (Eloff, Eloff 2005). The phases are summarised as follows (Rees, Bandyopadhyay & Spafford 2003):

- *Assess* – involves the sub-steps of policy assessment and risk assessment (conducting security assessments and business risks).
- *Plan* – focuses on activities such as policy development, security strategy creation and requirements definition.
- *Deliver* – key activities include controls selection and definition, evaluation, testing and implementation of controls.
- *Operate* – the sub-activities in this phase include monitoring of operations, ensuring compliance, identification of internal and external trends and management of events.

5.4.7 Sherwood Applied Business Security Architecture (SABSA)

SABSA is a framework and methodology for enterprise security architecture and service management. It is used for developing risk-driven enterprise information security

architectures and for delivering security infrastructure solutions that support critical business initiatives (SABSA 2011). The primary characteristic of the SABSA framework is that everything must be derived from an analysis of the business's requirements for security, in order to allow the organisation to develop and exploit new business opportunities (SABSA 2011).

The model is layered, with the top layer being the business requirements definition stage. At each of the lower layers a new level of abstraction and detail is developed through the definition of the conceptual architecture, logical services architecture, physical infrastructure architecture and, finally, to the lowest layer, the selection of technologies and products (component architecture) (SABSA 2011).

SABSA comprises four phases:

- *Strategy and planning.* This phase is about establishing context and focusing on activities, which include identifying business attributes, setting risk appetite, identifying risks and evaluating the risks (Sherwood, Clark & Lynas 2009).

- *Design*. In the design phase, the SABSA framework is concerned with issues such as business processes, business systems, staffing models and the design of internal controls (Sherwood, Clark & Lynas 2009).

- *Implement*. This phase addresses matters involving change management, project management and implementation of business systems, among other things (Sherwood, Clark & Lynas 2009).

- *Manage and measure.* During this phase, management of resources and processes is the area of focus. It addresses the items involved in performance management and risk monitoring (Sherwood, Clark & Lynas 2009).

5.4.8 Zachman Framework

The Zachman Framework is a framework for enterprise architecture, which provides a formal and highly structured way of viewing and defining an enterprise (Alghamdi 2010). It is

based on a two-dimensional classification matrix: one dimension of the Zachman classification matrix is based on six interrogatives (What? How? Where? Who? When? and Why?), while the other dimension is based on six stakeholder groups (Visionary, Owner, Designer, Builder, Implementer and Worker) (Zachman 2011). The classification matrix is intended to provide a holistic view of the enterprise architecture being modelled (Alghamdi 2010).

5.4.9 Octave

Octave is a methodology used for risk-based strategic assessment and planning for security (Alberts et al. 2003). Its main focus is on assets, threats and vulnerabilities (Vorster, Labuschagne 2005). In the Octave approach, the emphasis is on the use of internal people to lead the information security risk evaluation (Vorster, Labuschagne 2005, Alberts et al. 2003)(Alberts et al. 2003)(Alberts et al. 2003). Octave is suitable for large organisations (Alberts et al. 2003).

Octave is based on three aspects, namely, operational risk, security practices and technology (Alberts et al. 2003). These are complemented by a three-phased approach. These phases are the following (Alberts et al. 2003):

- **Phase 1.** Build asset-based threat profiles.
- **Phase 2.** Identify infrastructure vulnerabilities.
- **Phase 3.** Develop security strategy and plans.

5.4.10 Information Security Risk Analysis Method (ISRAM)

ISRAM is a survey-based model that uses a quantitative approach to risk analysis which allows for the participation of managers and staff in the organisation (Vorster, Labuschagne 2005). Quantitative tools included in ISRAM are simple numbers related to the survey, risk tables, as well as addition, multiplication and division operations (Karabacak, Sogukpinar 2005).

5.4.11 Cost of Risk Analysis (CORA)

In terms of CORA methodology, risk parameters are expressed quantitatively and losses are expressed in quantitative monetary terms. This framework uses data collected on items such

as threats, functions and assets, and calculates the losses that result from the occurrence of threats (Vorster, Labuschagne 2005).

5.4.12 Basel II

The Basel II framework was developed with the intention to improve the safety and soundness of the financial system by placing more emphasis on banks' own internal control and management, the supervisory review process and market discipline (Basel Committee 2001). The Basel framework focuses on risk management at banks.

The framework is structured into three main pillars (Basel Committee 2001):

- **First pillar:** minimum capital requirement
- **Second pillar:** supervisory review process
- **Third pillar:** market discipline

One of the components of the first pillar is the operational risk. Operational risk is defined as "the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events" (Basel Committee 2001). Based on this definition, information technology and information security risks fall under operational risk (IT Governance Institute 2006).

The Basel framework approach has been designed to encompass the complexity that is inherent in information technology (IT Governance Institute 2007b). Subsequently, the Basel II requirements have had a significant impact on the IT processes and infrastructure of financial institutions (Guldentops 2004). Examples of these would include business continuity, outsourcing, the adequacy of major IT investments, system obsolescence and the exposure of valuable and sensitive information (Guldentops 2004).

5.4.13 COSO ERM

An Enterprise Risk Management – Integrated Framework was issued by the Committee of Sponsoring Organisations (COSO) of the Treadway Commission with a view to assisting organisations to assess and enhance their internal control systems (COSO 2004a). COSO provides the basis for planning, designing and implementing a risk management framework in organisations that addresses both financial and operational risks (IT Governance Institute

2007b). Such a framework focuses on four dimensions of an organisation's objectives, namely, strategic, operations, reporting and compliance (COSO 2004a).

These four dimensions are divided into eight interrelated components, namely, internal environment, objective setting, event identification, risk assessment, risk response, information and communication, control activities and monitoring (COSO 2004a).

The COSO framework appeals to various stakeholders with an interest in enterprise risk management, including the board of directors, senior management, auditors and regulators (COSO 2004a).

5.2 Evaluation of existing frameworks

In the preceding sections, existing frameworks were examined and their purpose, domains and target audience discussed. It should be noted that, in terms of information security, these frameworks all have strengths and weaknesses. This section looks at those strengths and weaknesses.

The first framework to be evaluated is ISO/IEC 27002. The **ISO/IEC 27002** is an exclusive information security framework. It is more detailed (and more technically oriented) than COBIT and therefore provides more guidance on how things should be done (Von Solms 2005). Owing to its design, the ISO/IEC 27002 appeals more to information security professionals than to ICT security auditors and regulatory officials. ISO/IEC 27002 may also be viewed as 'stand-alone' guidelines that are not integrated into a wider framework for IT governance (Von Solms 2005).

The **Standard of Good Practice for Information Security** designed by the Information Security Forum (ISF) has good generic information security principles that can be used by any organisation to implement an information security programme. Since its scope is broad enough to cover a wide range of information security aspects, it appeals to various stakeholders, thus making it a good standard. However, it also has some limitations since it is for the exclusive use of members of the ISF.

The **PCI DSS** is only applicable to financial institutions that store, transmit and process credit card information. Its scope is therefore limited to financial institutions that have credit card processing systems.

While **COBIT** is a useful framework for identifying critical gaps, it has some deficiencies in that it offers minimal help in identifying the best practices that should be used to bridge those gaps (Fabian 2007). The reason behind this is that COBIT is a control and management framework rather than a process framework (IT Governance Institute 2008a). COBIT is also not an exclusive information security framework; it is an overall IT governance framework that encompasses many other things besides information security (Von Solms 2005). In terms of this study, the key advantage of COBIT is that it is acceptable to IT Security auditors, information security professionals and regulatory officials alike (IT Governance Institute 2007a).

The **ITIL** is strong in IT processes, but limited in security and system development (Hoekstra, Conradie 2002). Unlike the COBIT and ISO 27002, it provides the *how* part of IT service management (IT Governance Institute 2008a).

The **PFIRES**'s key strength is that, through four of its phases, it uses a life cycle in line with the standard information technology lifecycle (Rees, Bandyopadhyay & Spafford 2003). The downside of the model is the fact that it is relevant to strong security matters pertaining to e-commerce and security policy only. Its scope is therefore limited since information security is much broader than just these two areas.

The **SABSA** framework is business-driven and business-focused. It is also scalable, that is, it can be introduced in subsequent areas and systems and implemented incrementally (Sherwood, Clark & Lynas 2009). SABSA fills the gap for security architecture and security service management by integrating seamlessly with other standards such as The Open Group Architecture Framework (TOGAF) and ITIL (Sherwood, Clark & Lynas 2009). However, it only appeals to information security professionals.

The advantages of the **Zachman** framework approach include an intuitive classification matrix which provides comprehensive coverage for all enterprise architecture stakeholders (Alghamdi 2010). The weaknesses of the approach include the generation of voluminous specification documentation which can be of questionable utility (Alghamdi 2010).

OCTAVE, **ISRAM**, **CORA, Basel** and **COSO** are all focused on risk management, therefore they are rich tools for identifying risks, including those related to information security.

OCTAVE is an effective information security risk evaluation that considers both organisational and technological issues (Alberts et al. 2003). Such an evaluation is vitally important to any security-improvement initiative because it generates an organisation-wide view of information security risks, providing a baseline for improvement (Alberts et al. 2003). The limiting factors of the OCTAVE risk analysis methodology include, among others, a great deal of investment in time, resources and formal training (Abdullah 2006).

The key advantage of **ISRAM** is that it is easy to use and does not contain complicated mathematical and statistical instruments (Karabacak, Sogukpinar 2005). By contrast, **CORA**, because of the complexity and formality of its method, may require the participation of expert risk analysts (Karabacak, Sogukpinar 2005). CORA is also ideally suited for large organisations (SoftScout 2011).

Basel II and **COSO** are general risk management frameworks, with Basel being tailored for banks in particular. Although neither Basel nor COSO specifically address information management and information technology, their principles have an impact on information and related technology (IT Governance Institute 2007b).

The table below summarises the frameworks and standards that have been examined in the preceding section.

Table 5.1 Comparison of different frameworks and standards

	ISO/IEC 27002	ISF	PCI-DSS	COBIT	ITIL	PFIRES	SABSA	ZACHMAN	OCTAVE	ISRAM	CORA	BASEL II	COSO ERM
Area	Information security	Information security	IT Security	IT governance	IT service management	Information security	Architecture (information security)	Enterprise architecture	Risk management	Risk management	Risk management	Risk management	Risk management
Type	Standard	Standard	Standard	Framework	Framework	Framework	Framework	Framework	Standard	Framework	Standard	Framework	Framework
Focus	How	How	How	What	How	What	What	What	How	How	How	Compliance	Guideline
Level of applicability	Tactical	Tactical	Operational	Strategic	Tactical	Strategic	Strategic	Strategic	Strategic	Tactical	Tactical	Strategic	Strategic
Appeals to (role players)	Information security professionals	Information security professionals	Information security professionals	Information security professionals, ICT security auditors and regulatory officials	Information security professionals and ICT security auditors	Information security professionals	Information security professionals	Information security professionals and ICT security auditors	Information security professionals and ICT security auditors	Information security professionals and ICT security auditors	Information security professionals and ICT security auditors	Information security professionals, ICT security auditors and regulatory officials	Information security professionals, ICT Security auditors and regulatory officials
Key strength(s)	It is more detailed (and more technically oriented), it therefore provides more guidance on how things must be done.	Its scope is broad enough to cover a wide range of information security aspects; it appeals to various stakeholders	It provides a baseline of technical and operational requirements.	It is useful in identifying critical gaps in an IT environment. It brings IT closer to business by focusing on IT governance and corporate	It is a comprehensive framework regarding service management. It provides the 'how' part in the service manageme	It uses a life cycle through its four phases in line with the standard information technology lifecycle.	It is business driven and business focused. It integrates well with other standards and frameworks such as ITIL	It provides for intuitive classification matrix which provides comprehensive coverage for all enterprise architecture stakeholders.	It considers both organisational and technological issues.	It is easy to use and does not use complicated mathematical formulas.	It is ideally suited for large organisations.	It addresses risks more comprehensively.	It is a comprehensive and overall enterprise risk management framework.

Current Information Security Frameworks

	ISO/IEC 27002	ISF	PCI-DSS	COBIT	ITIL	PFIRES	SABSA	ZACHMAN	OCTAVE	ISRAM	CORA	BASEL II	COSO ERM
				governance	nt		and COBIT.						
Key weakness(es)	It is a standalone security standard.	The standard is for the exclusive use of ISF members.	It is only applicable to entities involved in payment card processing.	It is thin on details regarding "how" things should be done. It is not an exclusive information security standard.	It is limited in the area of information since it focuses more on IT processes.	It is strong only on security matters concerning e-commerce related and security policy.	It only appeals to information security professionals.	The weakness of the approach includes the generation of voluminous specification documentation which can be of questionable utility (Alghamdi 2010)	It requires a great deal of investment in human time, resources and formal training.	It is only focused on the risk management aspect of information security.	It may require the participation of expert risk analysts because of its complexity and the formality of its methods.	It is not Information security specific. Its target audience are financial organisations.	It is not Information security specific.

5.3 Conclusion

This chapter examined a number of common frameworks and standards. It also identified the strengths and the weaknesses of the frameworks. It was noted that, when frameworks are developed, they have a particular focus. Accordingly, it is should be expected that a single framework or standard cannot cover all aspects of information security and IT in general. What organisations usually do is to use a combination of different frameworks and standards to help them achieve various information security objectives.

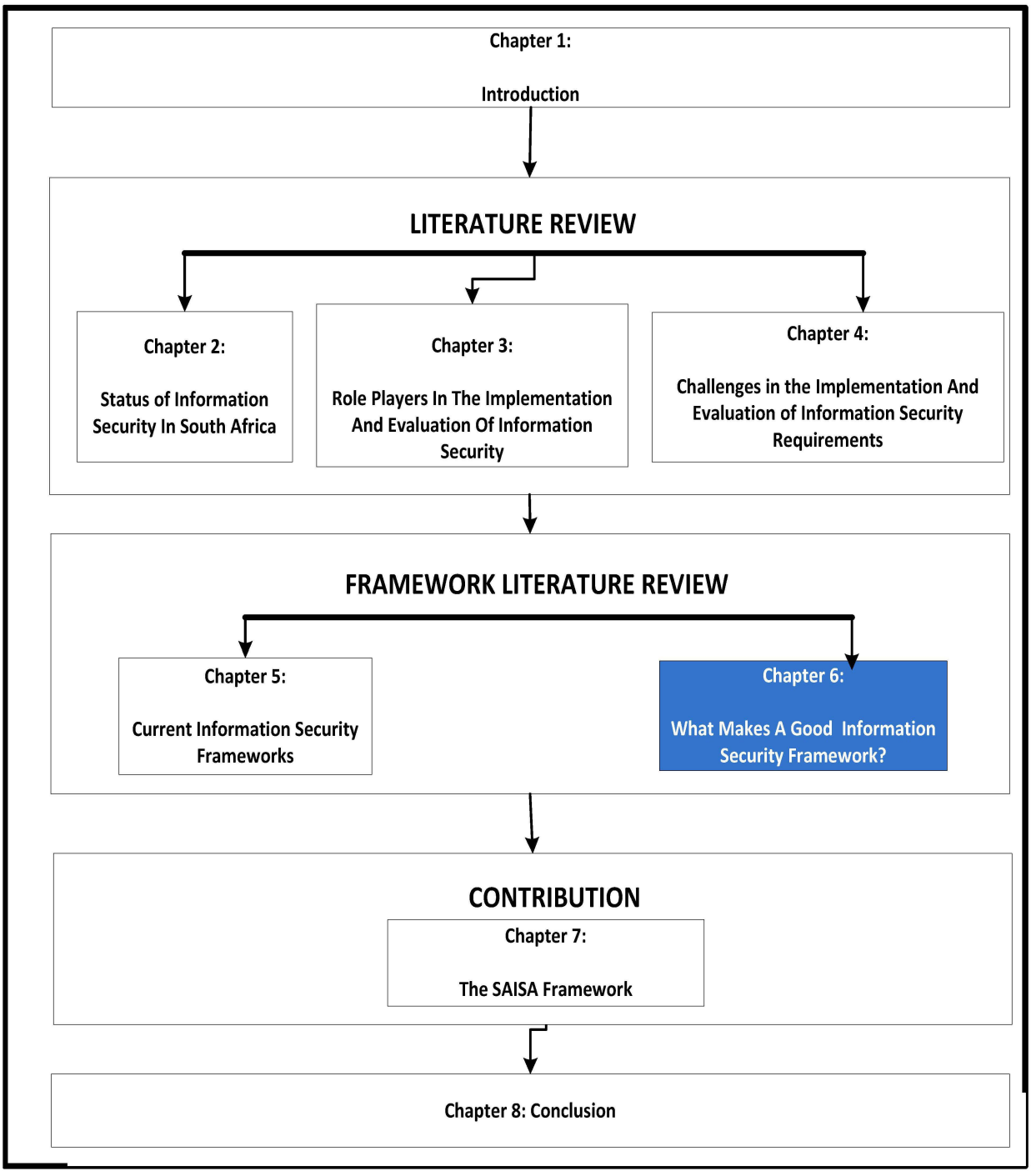
While there are various frameworks that can be used by different role players to implement and evaluate information controls, there is no framework that seeks to bring the three role players together in implementing and evaluating information security controls. The frameworks discussed in this chapter would allow for use by each role player independently of other role players; however, this could lead to a 'silo' effect, whereby the information security professionals and others parties involved (ICT security auditors and regulatory officials) would all be acting independently. This approach might be counterproductive since it does not ensure that there is alignment among the role players in relation to implementing and evaluating information security controls. For this reason, the role players should be aligned from the planning phases of information security up to the point where it is implemented and eventually evaluated. Consequently, there is a need to bring the role players together by using a framework that addresses the expectations and requirements of each role player. This will not only make the work of the role players easier, but it also has the potential to help organisations to implement sound information controls.

The establishment of the new framework does not seek to reinvent the wheel by trying to explore areas that have already been addressed by the existing frameworks. The framework will instead build and expand on that work.

The next chapter looks at the attributes of the various frameworks so that an understanding of what makes a good framework can be reached. These attributes will then form part of the new SAISA framework.

Chapter 6

What Makes A Good Information Security Framework?


Chapter 1:
Introduction
LITERATURE REVIEW
Chapter 2:
Status of Information Security In South Africa
Chapter 3:
Role Players In The Implementation And Evaluation Of Information Security
Chapter 4:
Challenges in the Implementation And Evaluation of Information Security Requirements
FRAMEWORK LITERATURE REVIEW
Chapter 5:
Current Information Security Frameworks
Chapter 6:
What Makes A Good Information Security Framework?
CONTRIBUTION
Chapter 7:
The SAISA Framework
Chapter 8: Conclusion

6.1 Introduction

The focus of the previous chapter was on various existing frameworks and standards for information security locally (South Africa) and internationally. The weaknesses of these frameworks were identified; however, such weaknesses may be as a result of the fact that each framework has its own focus areas. Following the discussion in the previous chapter, the proposed information security framework seeks to build on and enhance the work that has already been done on existing frameworks. This will be achieved by taking advantage of the strengths of existing frameworks while seeking to improve on the weaknesses as far as the alignment of ICT security auditors, information security professionals and regulatory officials in the implementation and evaluation of information security controls is concerned.

This chapter will highlight the components and attributes that make a good information security framework. This will be achieved by looking at critical components and attributes of the existing frameworks. These elements will then underpin the proposed framework, that is, they will be incorporated in the new framework.

6.2 Attributes of the information security framework

This section looks at the common characteristics of the various frameworks studied in chapter 5. These characteristics will be discussed under the following headings: the information security life cycle, critical elements of the framework, and the clarification of the roles and responsibilities of the stakeholders participating in a framework. These will now be discussed in detail.

6.2.1 Information security life cycle

In order to ensure that all aspects of information security are considered, it is essential that a framework follow an approach based on a comprehensive life cycle. The common life cycle approach adopted by most frameworks is one that is based on the plan–do–check–act (PDCA) cycle (Wright 2008, Eloff, Eloff 2005)(Wright 2008, Eloff, Eloff 2005), also commonly known as the Deming cycle (Vinh, Grewal 2005). It should be borne in mind that security is a

process and not a product; therefore, the life cycle approach should also be taken to managing security effectively, that is, organisations have to strive to constantly improve security (Vinh, Grewal 2005).

This life cycle contributes to ensuring that there is continuous improvement in a process by looking at its critical phases. The four phases referred to in a PCDA model can be summarised as follows:

- *Plan* – seeks to establish the strategies, objectives and programmes relevant to managing risk and improving information security, with a view to delivering results in accordance with an organisation's overall strategic direction and objectives (Nonaka 2009).

- *Do* – implement and operate the information security policy, controls, processes and procedures (Nonaka 2009).

- *Check* – assess and, where applicable, measure process performance against information security strategy and objectives and report the results to management for review (Nonaka 2009). This may involve the facilitation of audits to determine conformance to the statement of applicability and to identify opportunities for improvement (ISACA 2008b).

- *Act* – take corrective and preventive actions, based on the results of audits, evaluation, compliance monitoring or management review, in order to achieve continual improvement of information security (Nonaka 2009).

The PDCA model is illustrated in figure 6.1 below:

Figure 6.1 PDCA model (PDCA 2003)

Most information security standards and frameworks adopt the principles of the PDCA model in one form or another. A number of examples to this effect are discussed in the following paragraphs.

ISO/IEC 27001 is based on the PDCA approach (see figure 6.2) to modelling all information security management systems (ISMS) (ISO/IEC 27001 2005). The standard has the following phases that are in line with PDCA principles (ISO/IEC 27001 2005):

- Establish ISMS (plan).
- Implement and operate the ISMS (do).
- Monitor and review the ISMS (check).
- Maintain and improve the ISMS (act).

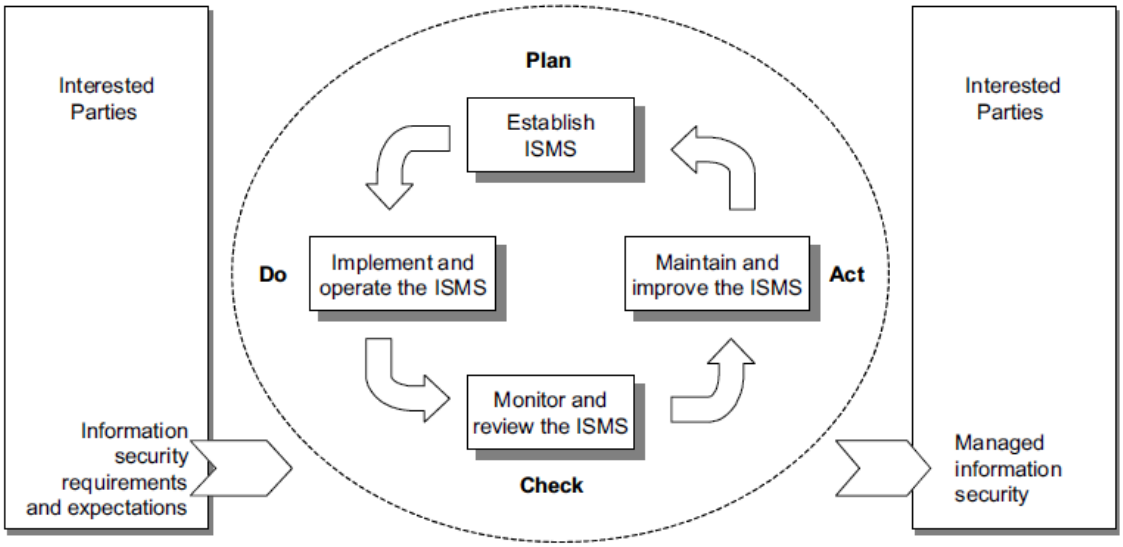


Figure 6.2 PDCA model applied to ISMS processes (ISO/IEC 27001 2005)

COBIT also has a structure similar to the PDCA model. The four COBIT domains (briefly discussed in chapter 5) demonstrate COBIT's resemblance in structure to that of the PDCA model (IT Governance Institute 2007a):

- *Plan and organise* – This domain focuses on strategy and tactics, and suggests ways in which IT can best contribute to the achievement of the business objectives. To realise strategic vision, it needs to be planned, communicated and managed according to different perspectives (ISACA 2008b, IT Governance Institute 2007a).

- *Acquire and implement* – To deliver on the IT strategy, IT solutions need to be identified, developed or acquired, as well as implemented and integrated into the business environment. In addition, changes in and maintenance to existing systems are covered by this domain to make sure that the life cycle is continued for these systems (ISACA 2008b, IT Governance Institute 2007a).

- *Deliver and support* – In this domain, the actual delivery of required services is addressed. These services range from traditional operations for security and continuity aspects to training. The delivery of services requires that the necessary support processes be put in place (ISACA 2008b, IT Governance Institute 2007a).

- *Monitor and evaluate* – All IT processes need to be assessed regularly over time for their quality and their compliance with control requirements. Thus, this domain addresses management's monitoring and evaluation of IT performance and increased control, ensuring regulatory compliance and providing IT governance oversight (ISACA 2008b, IT Governance Institute 2007a).

The ISO/IEC 27001 standard and COBIT are not the only frameworks/standards that have adopted the PDCA model. Other frameworks have followed suit and their structures also reflect PDCA principles. These include the approach that underpins the Sherwood Applied Business Security Architecture (**SABSA**), the Policy Framework for Interpreting Risk in E-Business Security (**PFIRES**) and **ITIL**.

The SABSA life cycle, shown in figure 6.3 below, is designed to align with the IT life cycle (SABSA 2011). In SABSA's life cycle, the first two phases of the SABSA development process are grouped in an activity called 'strategy and concept' (ISACA 2008a, Sherwood, Clark & Lynas 2009). This is followed by an activity called 'design,' which embraces the design of the logical, physical, component and operational architectures (ISACA 2008a, Sherwood, Clark & Lynas 2009). The third activity is 'implement' followed by 'manage and measure'. The significance of the 'measure' activity is that, early in the process, target performance metrics are developed as shown in the attributes section below (ISACA 2008a). Once the system is operational, it is essential to measure actual performance against targets, and to manage any deviations observed. Such management may simply involve the manipulation of operational parameters, but it may also feed back into a new cycle of development (ISACA 2008a).

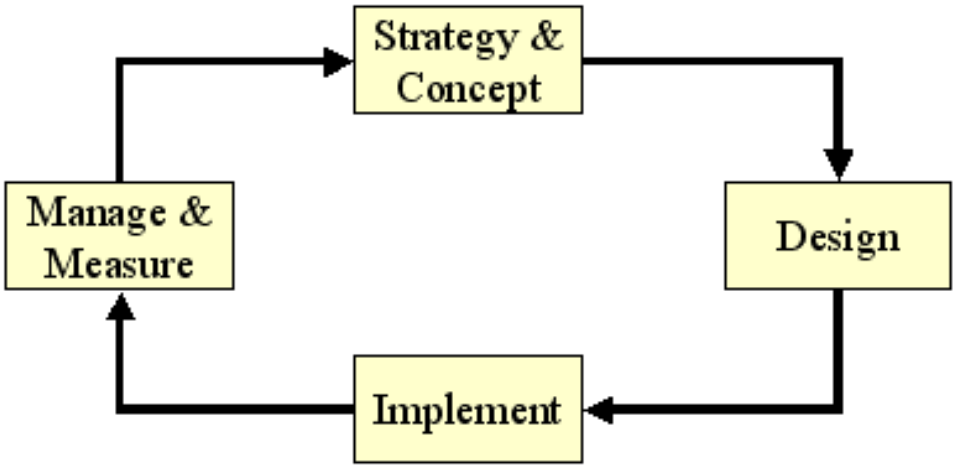


Figure 6.3 SABSA framework life cycle

The **PFIRES** life cycle consists of four major phases: *assess*, *plan*, *deliver*, and *operate*. Each is sharply defined with specific exit criteria that should be met before transitioning to the next phase (Rees, Bandyopadhyay & Spafford 2003).

ITIL's life cycle, which closely resembles the PDCA model, is as follows: *requirements, design, build, deploy, operate and optimise* (Rudd 2004). This is an end-to-end life cycle, which has clear stages that must be followed as the organisation embarks on implementing the ITIL.

The above discussion on the various frameworks and standards sought to indicate that they (frameworks and standards) have a common principle in their structure, that is, a life cycle. A life cycle ensures that there is a structure that is being adhered to by the framework, which ultimately facilitates the fulfilment of user requirements. For instance, the ISO/IEC 27001 standard adopts the PDCA lifecycle in order to take the information security requirements and expectations of the interested parties as input (ISO/IEC 27001 2005). By applying the required actions and processes, it produces information security outcomes that meet those requirements and expectations (ISO/IEC 27001 2005).

Critically, the life cycle allows for various role players to be involved in different stages of the framework. It could allow for the involvement of information security professionals, ICT security auditors and regulatory officials in the implementation and evaluation of information security controls in an organisation at various stages. For example, ICT security auditors can be involved in the planning and design stages of an information security

programme. If they have concerns they want to raise or contributions to make, they would do so there and then, before the information security professionals go ahead with implementing the security controls. This involvement could also help the auditors to adjust their audit programmes accordingly; moreover, it would help information security professionals to understand the expectations of the auditors. It is therefore clear that for a framework to be effective it must follow a proper approach based on a life cycle.

6.2.2 Critical elements of an information security framework

A framework must integrate certain elements to enable it to be more effective when it is applied in a real-world situation. The elements of the framework make it rich in detail and more meaningful to its users. Attributes such as inputs and outputs, measures and metrics have been found to prevail in most of the frameworks studied in chapter 5. In the same vein, certain questions (What? Why? How? and Who?) must be answered during the formulation of the framework (Sherwood, Clark & Lynas 2009, Zachman 2011). Answering these questions assists in the development of a comprehensive framework.

The elements and attributes of the critical elements of a framework will now be discussed:

- *Inputs and outputs.* Every process in a framework must have some sort of input and output (IT Governance Institute 2008b). Inputs are items that the process requires before it can be activated, while outputs refer to the outcomes and deliverables of the process. The output of one process can be an input to another process, especially in life cycle based processes. The COBIT framework uses inputs and outputs in all its processes.

- *Measures and metrics*. It is very important to have a means of measuring a particular activity, as this makes it easier to manage. The organisation's information security processes must be documented, measured and managed in order for them to be effective (The Open Group 2011). Measures and metrics are fundamental in providing decision support (ISACA 2008b), while KGIs and KPIs can be useful in determining whether a process has achieved its goal (ISACA 2008b).

- *Dependencies*. In order for a certain process to execute properly, certain conditions have to be satisfied. These conditions may not necessarily be in the control of the owner of the process.

- *What?* This, in the main, refers to the assets that need to be protected. It also refers to the business's needs for information security, for example security as a strategic business component, operational continuity or compliance with laws (Sherwood, Clark & Lynas 2009).

- *Why?* The reasons and motivation behind putting a particular control for information security in place. Answering the "Why" helps to indicate how important the control is in relation to the business objectives.

- *How?* This section describes how the protection will be achieved, in terms of high-level technical and management security strategies, as well as the tools to be used to meet the information security objectives from a business point of view (Sherwood, Clark & Lynas 2009)(Sherwood, Clark & Lynas 2009).

- *Who?* Specifying the entities (e.g. users, information security officers, compliance officers and auditors) and their interrelationships, attributes and authorised roles (Sherwood, Clark & Lynas 2009).

The above are not the only elements that are crucial in a framework. There are others that are equally important e.g. responsible, accountable, consulted, and informed. These are discussed in the following section.

6.3 RACI Model

The RACI (Responsible, Accountable, Consulted, and Informed) Model is a tool used for identifying and clarifying the roles and responsibilities in a process (RACI Model 2011). It is a two-dimensional matrix which shows the 'level involvement' of functional roles in a set of activities (Continental Solutions 2011). It is a powerful tool and can be used to determine the fundamental issues with a process where the wrong people are involved and/or no one

is accountable (Banacorsi 2011). The benefits of using the RACI Model are the following (Banacorsi 2011):

- Encourages teamwork by clarifying roles and responsibilities
- Eliminates duplication of effort
- Reduces misunderstanding
- Improves communication – makes sure people are not left out
- Determines ownership
- Helps clarify activities and tasks in a process
- Reduces bad decisions by ensuring the correct people are involved
- Clarifies hands-offs and boundaries
- Improves cross-functional view for all employees

RACI stands for Responsible, Accountable, Consulted and Informed:

- **R** = **Responsible**

The responsible person is the owner of the problem, activity or process (RACI Model 2011). The responsible individual performs an activity (the doer). The degree of responsibility is defined by the accountable person. Responsibility can be shared or delegated (Banacorsi 2011).

- **A** = **Accountable**

Accountable is the person to whom 'R' is accountable. They must sign off (approve) on the task before it is effective (RACI Model 2011). There can only be one accountable in a process and it cannot be delegated (Banacorsi 2011).

- **C** = **Consulted**

The consulted has the information and/or capacity necessary to complete the activity (RACI Model 2011). They are consulted before a final decision or action is taken (Banacorsi 2011).

- **I** = **Informed**

These are the individuals that must be notified after the action has been taken or, finally, of the results, but they need not be necessarily consulted (RACI Model 2011, Banacorsi 2011).

Based on the above, the RACI model can play a crucial role in ensuring that the roles and responsibilities of the information security professionals, ICT security auditors and regulatory officials are clarified and duplication of effort minimised or eliminated. Since the study is about these three role players, understanding and clarifying their roles and responsibilities is a key deliverable of this study. The RACI model helps in clarifying the roles and responsibilities of the role players in order to reflect the principle that the information security professionals have an operational role, while the ICT security auditors and regulatory officials, in contrast, have control responsibilities but not operational responsibilities (IT Governance Institute 2007a). Understanding the roles and responsibilities for each process is crucial for effective governance (IT Governance Institute 2007a).

6.4 Conclusion

It is clear that common attributes are found in the various frameworks. The life cycle was identified as one of the key structures that a framework should contain. The life cycle is important because it puts the structure in place that allows the framework to contain a number of phases that, when put together, form a complete cycle. Furthermore, it allows the framework to be organised into logical phases, starting with the planning phase and progressing to the phases that involve the implementation and measurement of programmes. The PDCA model was identified as the foundation of the life cycles adopted by many of the frameworks studied.

This chapter also discussed the critical elements that must be incorporated in a framework. These included items such inputs, outputs, measurements and metrics. Each phase in a life cycle must address the elements of the framework; this helps to divide the phases into

smaller building blocks that are easy to work with. Elements common to many frameworks were briefly defined and discussed.

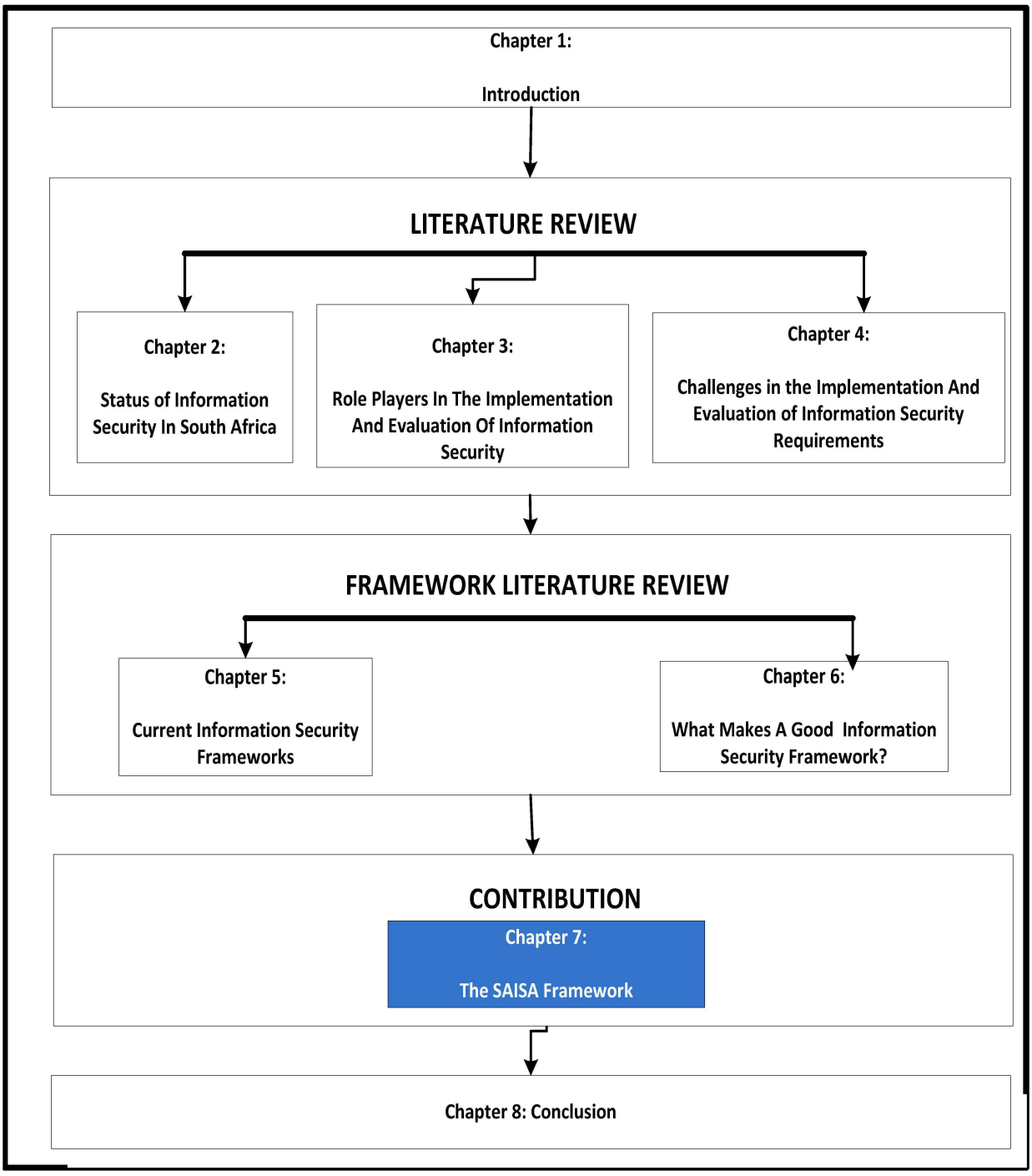
The RACI model, which is used to identify and clarify roles and responsibilities, was discussed. The discussion focused on how the RACI model can assist in ensuring that the role players understand what is expected of them within a framework.

The following chapter will present the proposed framework. In line with the characteristics of the frameworks studied, the new framework will comprise the four phases that have been identified as making up a life cycle. Each phase will consist of elements that are in line with the practices adopted by the various frameworks. The roles and responsibilities of the role players in each phase will be clarified by applying the RACI model.

Chapter 7

The SAISA Framework

The SAISA framework



7.1 Introduction

In the previous chapters, the focus was on literature concerning the general information security position in South Africa and abroad. The initiatives and solutions that currently exist in this regard were identified and discussed. In addition, the current challenges (such as lack of skills, financial resources constraints) faced by those with an interest in information security were highlighted. It was also acknowledged that information security requires support and commitment, as well as the involvement of many role players in an organisation. However, for the purposes of the study, the focus is on the involvement of the three key role players in the sphere of information security. These are information security professionals, ICT security auditors and regulatory officials.

The three role players were identified as the critical stakeholders in the implementation and evaluation of information security. The preceding discussion has highlighted the fact that, although the three role players have their own distinct roles, their work is closely linked and therefore a great deal of integration and alignment is required. However, as was also mentioned, there is no framework that provides specific guidance on the way in which the three role players can be aligned in the implementation and evaluation of information security controls.

The identification of this misalignment problem led to a new approach being proposed to address this problem. The proposed approach takes the form of an information security framework, which will ensure alignment among information security professionals, ICT security auditors and regulatory officials. Although there is currently no specific framework that seeks to ensure alignment among the three role players, it should be noted that there are existing frameworks that in some way or another address this challenge, albeit on a limited scale (not comprehensively). To this end, the current information security frameworks had to be looked at with a view to identifying their strengths, weaknesses and general characteristics.

This chapter presents a new framework which is intended to ensure the alignment of information security professionals, ICT security auditors and regulatory officials in the implementation and evaluation of information security controls in organisations.

7.2 The South African Information Security Alignment (SAISA) framework

The main objective of this framework is to ensure alignment among information security professionals, ICT security auditors and regulatory officials in the implementation and evaluation of information security by South African organisations. The framework seeks to achieve this by involving all these role players in all stages of the information security programme, that is, from the planning phase, through its execution to, eventually, the evaluation of the information security controls.

This approach, which involves the role players in all stages of the information security programme, ensures that any gaps are highlighted as close as possible to the point where they occur. It is cheaper to correct gaps at this stage than to deal with them at a later stage, when it could even be too late.

The SAISA framework seeks to assist the three role players in the following ways:

- By ensuring that information security professionals are able to understand what is expected of them during the planning phases of information security programmes. This has a potential to produce fewer surprises at the end when the ICT security auditors and regulatory officials evaluate the controls and issue reports.

- By enabling ICT security auditors to understand the organisation's risk profile, as well as its capacity and capabilities. This will help them formulate their audit programmes in line with the information they obtain from the planning stages of the information security programme.

- By giving regulatory officials an opportunity to make information security professionals aware of what is expected of them with regard to regulatory compliance during the planning, implementation and delivery phases. This has the potential to improve compliance with regulatory requirements.

- By ensuring that the three role players engage with each other in all the phases of the programme. This approach helps all concerned to know what the other parties are doing and where necessary align appropriately. For example, if, during a risk assessment, information security professionals identify information leakages as the highest risk, then ICT security auditors can align the audit programme so that it focuses on the evaluation of controls related to information leakage. Furthermore, if regulatory officials have more concerns about privacy issues, the information security professionals can make privacy one of the key items to be addressed in an information security programme. In addition, the ICT security auditors would have to ensure that their audit programme address the evaluation of controls related to privacy matters.

It should be emphasised that ICT security auditors and regulatory officials must remain independent and this framework does not seek to change this. Although the planning, implementation and delivery of information security programmes are the primary responsibilities of information security professionals, during these stages, the ICT security auditors and regulatory officials play an advisory/support role and are able to collect information which also improves the quality of their own work. The ICT security auditors and regulatory officials are primarily responsible for monitoring and evaluating the information security controls, which is usually the last phase of the information security programme.

7.2.1 Structure of the SAISA Framework

Chapter 6 highlighted the fact that it is crucial for a framework to a follow a structured life cycle in the form of a PDCA model. Accordingly, the proposed framework will not deviate from this common practice, but will adopt the four COBIT framework domains. The COBIT framework is referred to as the overall IT governance framework. Through IT governance, information security forms part of corporate governance. Accordingly, COBIT is a framework that can be used by organisations to implement IT governance effectively in their environments.

The SAISA framework

This study does not seek to reinvent the wheel when it comes to the existing frameworks. Hence, it is essential to base the new information security framework on the existing framework(s) so as to capitalise on their strengths while seeking to establish a framework that aligns the role players in the implementation and evaluation of information security controls. A decision was therefore taken to base the new framework (structurally) on COBIT because of its IT governance coverage (information security is part of IT governance), its lifecycle approach and the fact that it appeals to all the three role players.

While COBIT is a high-level IT governance framework, it is not a framework that explicitly ensures the alignment of information security professionals, ICT security auditors and regulatory officials in terms of information security implementation and evaluation. The reason for this is, partly, that COBIT is not exclusive to information security – it addresses information technology governance and refers, among many other issues, to information security (Von Solms 2005).

As indicated in chapters 5 and 6, COBIT has four domains, namely: Plan and Organise (PO), Acquire and Implement (AI), Deliver and Support (DS), and Monitor and Evaluate (ME). The SAISA framework adopts these four domains from a structural point of view. As such, the new framework will have four phases that resemble the four COBIT 4.1 domains.

The SAISA framework, subsequently, has the following phases:

- Plan and organise information security (PO-IS)
- Acquire and implement information security AI-IS)
- Deliver and support information security (DS-IS)
- Monitor and evaluate information security (ME-IS)

The four phases of the framework seek to ensure the effective implementation and evaluation of information security. Each phase provides information on what is expected from each role player and what tools and approaches they can use to execute their tasks. The framework is illustrated in figure 7.1 below.

The SAISA framework

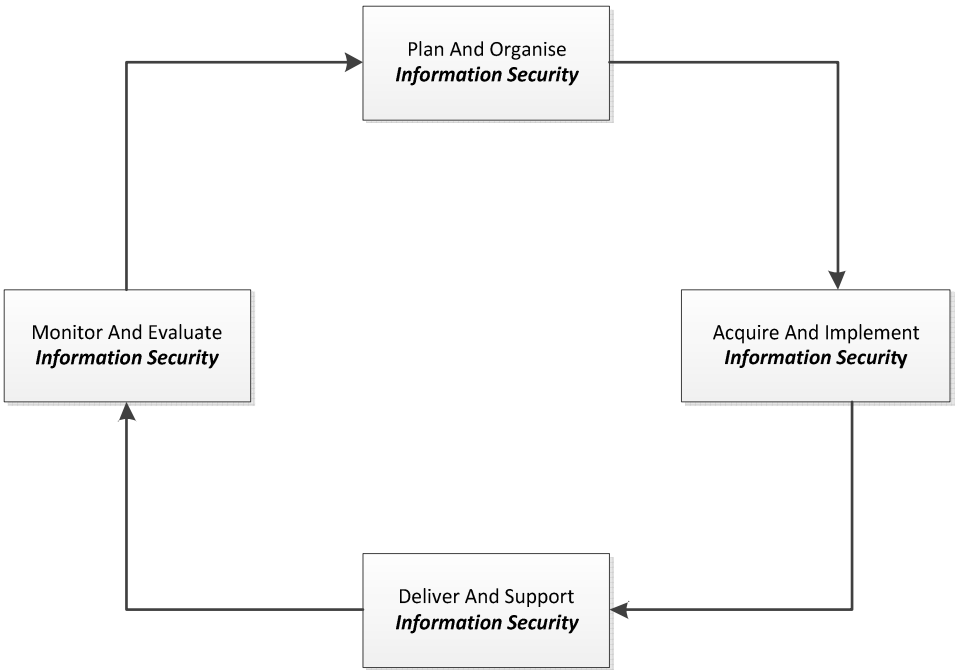


Figure 7.1 SAISA framework life cycle

7.2.2 Elements of the SAISA framework

Each phase of the SAISA framework has multiple key elements. These elements help to clarify what is expected from each role player in each phase of the framework. The elements have been adapted from those identified in chapter 6. In that chapter, the following were identified as being critical in a framework: What, Why, How, Who, Inputs and Outputs, Measures and Metrics, Dependencies and Level of involvement.

Based on these elements, the following have been identified as key elements of the new framework:

- Role
- Objective
- Approach
- Tools
- Level of involvement
- Dependencies
- Inputs
- Deliverables

- Measurements

These elements are discussed in detail below. The items in parenthesis indicate the relationship between the element and the ones identified in chapter 6.

Role (What & Who?)

The role for each role player in each phase is defined in this section. This is to ensure that each role player understands what is expected of them in the particular phase. It also helps each role player to understand the roles of the other role players in each phase.

Objective (Why?)

In the objective section, the reason behind each role player's involvement in each phase is defined. It is important for each role player to understand why the other role players are involved in each phase, as this can improve cooperation among the role players.

Approach (How?)

To achieve the objectives, certain approaches are necessary. A recommended approach is spelt out here. This approach provides the 'how' or the way in which each role player achieves their goals.

Tools (How?)

These are the minimum tools required for each role player to succeed in achieving their objectives and performing according to the role definition. These tools could be anything from automated systems to documented processes, standards and guidelines

Level of involvement (RACI Model)

This section seeks to define the level of involvement that is expected from each role player in each phase. There are two levels of involvement: primary involvement and secondary involvement. If the role player has a primary involvement in the phase, it means this phase forms the core of the role player's responsibility.

If the involvement of the role player is secondary, it means that the role player is playing an advisory/support role to ensure that the other role players are able to achieve their

objectives successfully. This involvement is still critical, however, because without their advice/support the other role players may not necessarily succeed.

A RACI model is used to define the roles in the form of Responsible, Accountable, Consulted and Informed.

Dependencies (Dependencies)

These requirements are not necessarily under the control of the role player, but are critical factors in ensuring that the role player is able to deliver on what is expected of them in the particular domain.

Inputs (Inputs)

These may be documents and any other information which are of use to the role player in understanding the environment so that they can formulate their plans and strategies better. This can also be information that the role player needs in order to make the appropriate choices and opinions regarding the controls. Inputs can either be internal (to the organisation) or external (e.g. regulatory requirements).

Deliverables (Outputs)

This is a list of deliverables, which is expected from the role player in each phase. Accordingly, the deliverables in one phase may be an input in the next domain. However, they could also be used by other role players in executing their activities.

Measurements (Measures and Metrics)

These are the measurement criteria of the deliverables expected from the role players in each phase.

7.2.3 RACI chart for the framework

A RACI model is used to determine the level of involvement for the role players. As already mentioned, **RACI** stands for: R = Responsible, A = Accountable, C = Consulted and I = Informed. In this study, RACI has been adopted for the framework to ensure that the roles and responsibilities of the role players are properly clarified. This is illustrated in table 7.1.

Table 7.1 RACI model For SAISA framework

Role Players	Information Security Professionals	ICT Security Auditors	Regulatory Officials	Comments
Phases				
Phase 1: **Plan and organise information security**	A/R	C	C	Information security professionals are accountable and responsible for the planning of information security. Auditors and regulatory officials are consulted.
Phase 2: **Acquire and implement information security**	A/R	C	I	Information security professionals are accountable and responsible for the implementation of information security. Auditors are consulted while regulatory officials are informed.
Phase 3: **Deliver and support information security**	A/R	C	I	Information security professionals are accountable and responsible for supporting information security (e.g. configuring firewalls). Auditors are consulted while regulatory officials are informed.
Phase 4: **Monitor and evaluate information security**	A	R	C	Information security professionals are accountable for addressing the findings of the auditors (who are responsible for evaluating the controls). Regulatory officials have to be consulted in order to ascertain that the compliance requirements are met by the organisation.

The detailed framework, complete with all the details, is presented in the next section:

7.2.4 The SAISA Framework

Table 7.2 The SAISA Framework

PHASE 1	**PLAN AND ORGANISE *Information Security***		
ROLE PLAYERS	**Information security professionals**	**ICT security auditors**	**Regulatory officials**
ELEMENTS			
Objective	▪ To ensure that the security programme is driven from a strategic point of view.	▪ To ensure that gaps in strategy are identified and highlighted at the very beginning before programme is implemented.	▪ Assist information security professionals to incorporate key regulatory requirements in to the strategy.
Role	▪ Develop information security strategy. ▪ Review information security strategy on an annual basis. ▪ Develop information security programme.	▪ Understand the information security strategy. ▪ Ascertain that the strategy is in line with corporate strategy.	▪ Highlight regulatory requirements that must be met by the organisation so that they can be incorporated into the strategy.
RACI Chart	▪ Accountable/responsible	▪ Consulted	▪ Consulted
Approach	▪ Perform risk assessments. ▪ Understand the business strategy and translate it into information security deliverables. ▪ Look at the previous ICT audit reports. ▪ Prioritise deliverables based on the business requirements.	▪ Understand the internal control model of the organisation. ▪ Read and assess the information security strategy.	▪ Provide a list of compliance requirements that are applicable to the organisation concerned. ▪ Educate information security professionals on what is expected of them to ensure compliance. ▪ Hold workshops, seminars and telephonic advice centres where regulatory requirements are discussed.

The SAISA framework

Tools	▪ ISO 27002 ▪ ITIL ▪ COBIT ▪ OCTAVE ▪ CORAS ▪ ISRAM ▪ CORA ▪ COSO	▪ COSO ▪ COBIT ▪ ISACA Standards and Guidelines ▪ Institute of Internal Auditors Standards ▪ General Accepted Auditing Standards	▪ ECT Act ▪ Comsec Act ▪ Electronic Communications and Transactions (ECT) Act ▪ Protection of Personal Information (PPI) ▪ Regulation of Interception of Communication Act (RICA) ▪ Financial Intelligence Centre Act (FICA)
Level of involvement	▪ This is the information security professionals' primary area. They need to develop and own the strategy.	▪ ICT security auditors play a supportive role in helping to ensure that the information security strategy has as few gaps as possible.	▪ Regulatory officials help to ensure that the strategy does not omit the key compliance issues. They play a supportive role.
Dependencies	▪ Senior management involvement	▪ Timely availability of information from those developing the strategy	▪ Willingness of the information security professionals to accept advice and incorporate it into the strategy
Inputs	▪ Corporate strategy ▪ Enterprise risk framework. ▪ ECT Act ▪ Comsec Act ▪ Electronic Communications and Transactions (ECT) Act ▪ Protection of Personal Information (PPI) ▪ Regulation of Interception of Communication Act (RICA) ▪ Financial Intelligence Centre Act (FICA) ▪ KING III ▪ ICT security auditors findings and recommendations ▪ Best practices ▪ Threats analysis	▪ Corporate strategy ▪ Information security strategy ▪ Previous audit reports	▪ COMSEC ▪ Cyber inspectors National Cyber Security Advisory Council ▪ National Computer Security Incident Response Teams

Deliverables	▪ Information security strategy. ▪ Information security implementation roadmap. ▪ Information Security Policies. ▪ Information security architecture. ▪ Risk Registers.	▪ Organisation's risk profile ▪ Audit programme	▪ List of laws applicable to the organisation ▪ List of compliance requirements
Measurements	▪ Completeness of the strategy ▪ Alignment of the strategy with the corporate strategy	▪ Audit programme based on the information security strategy and the organisation's risk profile	▪ Level of compliance of the strategy to the regulatory requirements
PHASE 2	**ACQUIRE AND IMPLEMENT *Information Security***		
ROLE PLAYERS	**Information security professionals**	**ICT security auditors**	**Regulatory officials**
ELEMENTS			
Objective	▪ Identification and implementation of appropriate systems in line with information security strategy must be performed by information security professionals.	▪ Having independent assurance in the project ensures deviations are strictly controlled and reported to the appropriate structures (e.g. project boards).	▪ The regulatory officials are appraised on the solutions obtained to ensure compliance with regulatory requirements.
Role	▪ Identify, acquire and implement the information security technologies.	▪ Provide assurance on information security projects.	▪ Advise on the suitability of the identified solutions for meeting the compliance requirements.
RACI Chart	▪ Accountable/Responsible	▪ Consulted	▪ Informed
Approach	▪ Employ the project management methodology to ensure that technology implementation subscribes to best practices.	▪ Review the solutions being implemented, identify and highlight any gaps. ▪ Verify that the project subscribes to best practices. ▪ Verify that the project undertaking is in line	▪ Compare the solution capabilities to the identified compliance requirements.

		with the information security strategy.	
Tools	▪ System Development Life Cycle (SDLC) processes. ▪ Project management tools ▪ Project management processes (e.g. PMBOK or PRINCE 2). ▪ Business cases	▪ SDLC processes ▪ Source code ▪ Computer Aided Audit Engineering Tools (CAAT's) ▪ Business cases. ▪ Project reports	▪ Business cases ▪ Project reports
Level of involvement	▪ Information security professionals are the primary owners of this process. They must identify, acquire and implement appropriate solutions in line with the strategy.	▪ The ICT security auditors must provide quality assurance to ensure that elements that may have adverse effects on the project are highlighted and reported on appropriately.	▪ Regulatory officials provide the advisory services only to information security professionals to ensure that the new technologies being implemented meet the compliance requirements.
Dependencies	▪ Funding availability ▪ Resources availability ▪ Project sponsor support	▪ Corporation from the project resources ▪ Timely availability of the information	▪ Corporation from the project resources ▪ Timely availability of the required information
Inputs	▪ Information security strategy ▪ Information security architecture ▪ Risk register	▪ Project plans ▪ Progress reports	▪ Business cases ▪ Technical assessment of the solution
Deliverables	▪ Information security standards ▪ Project scope ▪ Project report	▪ Project risk registers ▪ Auditors' project reports	▪ Reports on how the technology will meet the compliance issues. ▪ Reports on any possible gaps that the solution might have in relation to the compliance requirements.
Measurements	▪ Failure/success rates of the information security projects.	▪ Findings/gaps identified during project	▪ Completeness of the reports identifying the gaps between capabilities of the solution and the compliance requirements ▪

The SAISA framework

PHASE 3	**DELIVER AND SUPPORT *Information Security***		
ROLE PLAYERS	**Information security professionals**	**ICT security auditors**	**Regulatory officials**
ELEMENTS			
Objective	▪ Information security professionals must ensure that the deployed solutions run smoothly and are continuously maintained to stay abreast of the new requirements.	▪ ICT security auditors must provide independent assurance as to whether the changes to the production environment are introduced through a formal process (e.g. change management process).	▪ The regulatory officials must satisfy themselves that the deployed systems and processes ensure the organisation's compliance with regulatory requirements.
Role	▪ Ensure that information security systems run in accordance with information security requirements. ▪ Maintain the systems and the configurations. ▪ Maintain the appropriate documentation.	▪ Verify that the change management processes are being adhered to. ▪ Identify any deviations from the strategy.	▪ Ascertain that the delivered solutions ensure compliance with the provisions of the regulatory requirements.
RACI Chart	▪ Accountable/Responsible	▪ Consulted	▪ Informed
Approach	▪ Perform self-assessments ▪ Produce and react to performance reports of the systems.	▪ Continuous auditing	▪ Review the reports from the information security professionals on what is being done to ensure the systems' continuing complying with the regulatory requirements.

The SAISA framework

Tools	▪ Identity management ▪ User awareness ▪ Firewall ▪ Antivirus ▪ Passwords ▪ Physical security ▪ Vulnerability assessment tools ▪ Background checks	▪ Continuous auditing tools ▪ Vulnerability assessment tools	▪ Reports ▪ Compliance checklists
Level of involvement	▪ This is the information security professionals' primary are;, they are expected to deploy, support and maintain the systems and processes to stay abreast of new trends and developments inside and outside the organisation.	▪ The ICT security auditors must provide continuous assurance to ensure that the systems and processes continue operating efficiently and effectively.	▪ The regulators play a silent role, and are dependent on information security professionals and ICT security auditors for reports to determine systems' level of compliance. They may, however, conduct spot checks to ascertain that what is reported is in line with what is happening on the ground.
Dependencies	▪ Appropriately developed solutions to ensure reliability	▪ Appropriate access to the systems to allow for the running of the audit tools	▪ Completeness of the provided information by information security professionals and ICT security auditors
Inputs	▪ Information security standards	▪ Reports from auditing tools ▪ Reports from vulnerability assessments ▪ Information security standards, procedures, guidelines and processes	▪ Auditors reports ▪ Information security professionals reports ▪ Requested evidence
Deliverables	▪ Reports (e.g. incident reports) ▪ Trend analysis reports ▪ Information security procedures, guidelines and processes ▪ Operational manuals	▪ Preliminary findings ▪ Reports on the assessment and effectiveness of controls	▪ Preliminary compliance reports

Measurements	▪ Resilience and robustness of the systems ▪ Intrusion detection/prevention capabilities ▪ Level of security awareness within the organisation	▪ Quality of the preliminary findings ▪ Early detection of deviations	▪ Capability to identify and enforce compliance issues before they deteriorate further ▪ Level of compliance with the regulatory requirements of the organisation
PHASE 4	**MONITOR AND EVALUATE *Information Security***		
ROLE PLAYERS	**Information security professionals**	**ICT security auditors**	**Regulatory officials**
ELEMENTS			
Objective	▪ While independent reviews are performed by ICT security auditors, information security professionals must perform their own assessment in order to proactively rectify any deviations.	▪ This is the ICT security auditors' primary area and the reports they produce are used by senior management, the board, shareholders and other stakeholders in order to provide an understanding of the level of information security controls in an organisation.	▪ Regulatory officials need to determine whether the information security controls implemented in an organisation are in line with regulatory requirements. The officials produce reports detailing the level of compliance of the organisation. They also recommend punitive measures that the organisation must face when regulatory requirements are violated.
Role	▪ Monitor the implemented controls against the information strategy. ▪ Evaluate the information security strategy against the business strategy to ensure alignment and relevance.	▪ Provide an independent review of the implemented controls against the information security and corporate strategies. ▪ Provide the recommendations on corrective action to be taken by management. ▪ Perform follow-up audits	▪ Assess the state of compliance of the information security controls against the regulatory requirements. ▪ Assess the seriousness of violation, if any. ▪ Provide advice on the correct action to take. ▪ Advise on the punitive measures to be taken against the organisation in case of violations.

RACI Chart	▪ Accountable	▪ Responsible	▪ Consulted
Approach	▪ Perform proactive self-assessments on an ongoing basis with a view to taking corrective action where necessary.	▪ Request and review the evidence in order to ascertain whether the information security controls in an organisation are effective and efficient. ▪ Interview the information security professionals to gain more insight into the way controls are implemented and identify any gaps.	▪ Compare reports and evidence from information security professionals against the compliance requirements.
Tools	▪ Logs ▪ Incident reports	▪ Computer-Assisted Audit Techniques (CAATs) ▪ Evidence ▪ Working papers	▪ Compliance checklists ▪ Auditors' reports ▪ The reports received from information security professionals
Level of involvement	▪ Information security professionals play a mainly supportive role in this domain by providing the reports and evidence requested by the ICT security auditors and regulatory officials.	▪ As this is their core area, ICT security auditors must go through the evidence before them and state opinions on the adequacy of the information security controls. The auditors are therefore involved from start to finish in this phase.	▪ Regulatory officials can use the auditors' reports to gain a general understand of the information security controls in an organisation, especially in relation to compliance matters. If the auditors' reports highlight the possibility of serious breaches of regulatory requirements, the regulators may perform their assessments to determine if indeed there are any serious compliance issues.
Dependencies	▪ Facility to keep logs.	▪ Accessibility and readability of the logs ▪ Timely availability of the required evidence	▪ Completeness of the information provided by the information security professionals.
Inputs	▪ Audit logs (e.g. user activity) ▪ Reports e.g. from firewalls and antivirus	▪ General standards.	▪ Auditors' reports. ▪ The reports received from information

	servers	▪ Standards of field work ▪ Standards of reporting	security professionals ▪ Regulatory universe ▪ Previous reported issues
Deliverables	▪ Management comments (from the audits) ▪ Action plan for resolving the findings	▪ Conclusions ▪ Findings ▪ Recommendations ▪ Audit reports	▪ Final reports ▪ List of transgressions ▪ Recommendations ▪ Punitive measures
Measurements	▪ Number of new findings ▪ Number of repeat findings	▪ Quality of the findings ▪ Performance of the field work on time and on budget	▪ Enforcement of the compliance requirements

7.3 Conclusion

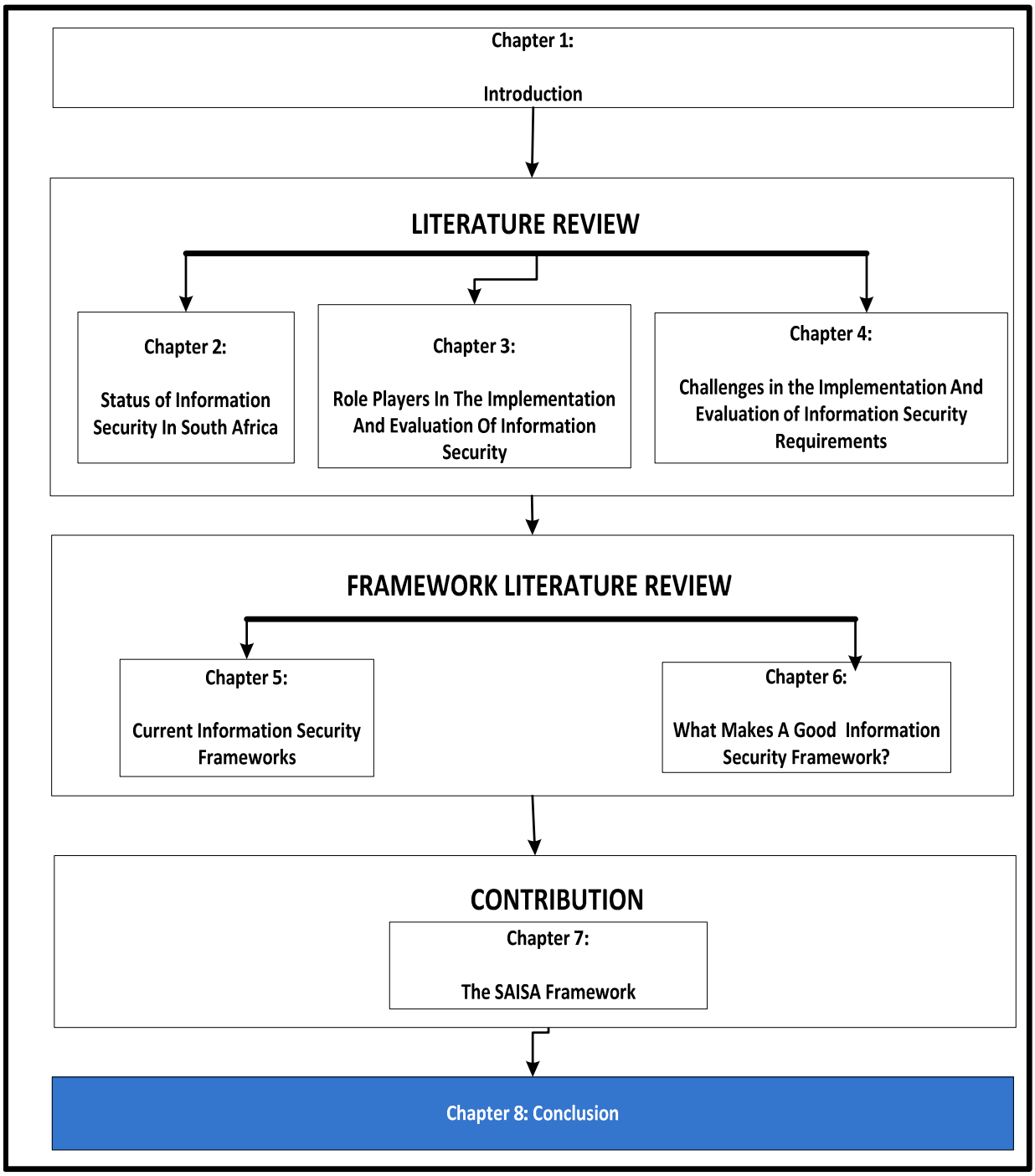
The above framework seeks to improve alignment among the three role players. It does not replace existing frameworks such as ISO 27002 and COBIT. In fact, it incorporates the existing frameworks and standards by recommending that they be used as tools for the planning and implementation of information security controls.

It should be noted that this framework is broad in nature. As such, certain elements may be adjusted depending on where it is applied. For instance, a financial institution may adjust it to fit the financial environment by removing the regulations and laws not applicable to financial institutions (e.g. RICA). Similarly, telecommunications organisations can remove the regulations and laws that are not applicable to the telecommunications industry (e.g. FICA and PCI DSS) from the framework. In essence, the framework provides a high-level guideline for ensuring the alignment of information security professionals, ICT security auditors and regulatory officials, as information security controls are implemented and evaluated. Using these guidelines, the framework can be easily adapted to various scenarios.

Chapter 8

Conclusion

Conclusion


Chapter 1:
Introduction
LITERATURE REVIEW
Chapter 2:
Status of Information Security In South Africa
Chapter 3:
Role Players In The Implementation And Evaluation Of Information Security
Chapter 4:
Challenges in the Implementation And Evaluation of Information Security Requirements
FRAMEWORK LITERATURE REVIEW
Chapter 5:
Current Information Security Frameworks
Chapter 6:
What Makes A Good Information Security Framework?
CONTRIBUTION
Chapter 7:
The SAISA Framework
Chapter 8: Conclusion

8.1 Introduction

The South African Information Security Alignment (SAISA) framework was presented in the previous chapter. This chapter revisits the objectives of this study, as outlined in chapter 1, in order to determine how they were met as the framework was established. The chapter also focuses on the research questions that underpin this study in order to ascertain how they were answered. Further, the strengths and the weaknesses of the framework are discussed and future work in this field is recommended.

8.2 Research objectives

The objectives of the research were to (a) identify the common areas among the role players; (b) identify the methodologies and tools of each role player, which they use to carry out their responsibilities; (c) bridge the gaps between the role players; (d) address the misalignment problem among the role players; and (e) establish a groundwork for a framework.

By means of a literature review, common areas among the role players were identified especially with regard to the fact that they all have one common goal: to ensure that the organisation's assets and the interests of various stakeholders (e.g. customers and shareholders) are properly protected. Standards and frameworks were also identified as areas of overlap among the role players. For instance, COBIT can be used by information security professionals to implement controls, while it can also be used by ICT security auditors to identify and evaluate controls. Regulatory officials can also use it to verify the compliance status of the organisation.

The tools and methodologies that are used by each role player were identified and discussed in chapter 3. These included audit standards and Computer Assisted Audit Tools (CAATS) for auditors, information security standards (e.g. ISO/IEC 27002) for information security professionals, and laws and legislation (e.g. ECT Act) for regulatory officials. The tools and methodologies were included as part of the SAISA framework.

The SAISA framework addresses the gaps among the role players, since all the parties become involved in all four phases of the framework. These phases broadly encompass the planning, implementation, support and evaluation of the information security programme. The involvement of the role players in the various stages of the information security programme also helps to ensure alignment among the role players.

Finally, the proposed framework was presented in chapter 7. This framework provides the groundwork for ensuring alignment among the three key role players in terms of the implementation and evaluation of information security controls.

8.3 Research questions

The study was based on the following four research questions:

- How can interpretation problems experienced by the role players relating to the implementation and evaluation of information security controls be prevented?
- What prioritisation challenges are faced by the role players?
- What can be done to establish a solution/delivery/measurement oriented approach to implement and evaluate information security controls?
- Are the roles of the three role players clearly defined and understood?

The following paragraphs discuss the way in which these questions were answered.

How can interpretation problems experienced by the role players relating to the implementation and evaluation of information security controls be prevented?

Since the role players are involved and interact with each other in all phases of the framework, the risk of varying interpretations of the information security requirements is minimised. If issues arise in any phase, they are addressed at that point. That is, they are resolved as close to where they occurred as possible. For instance, if a requirement during the planning phase is misinterpreted, the problem is resolved there and then, instead of moving on to another phase, such as implementation, without being resolved.

What prioritisation challenges are faced by the role players?

Having the role players involved in all the phases ensures that they all understand the capabilities of and the constraints on the organisation. Subsequently, they may understand the organisation's priorities on the basis of documents such as the business strategy and risk assessments. Therefore, when the ICT auditors and regulatory officials perform their assessments and evaluations they generally place more emphasis on the areas that have been prioritised instead of just performing tests arbitrarily.

What can be done to establish a solution/delivery/measurement-oriented approach to implementing and evaluating information security controls?

In each phase there are deliverables that are expected from each role player. The measurements to indicate the effectiveness of the deliverables are included in the framework. This ensures that the notion of merely providing the deliverable simply for the sake of 'ticking the box' is done away with. Each role player must have deliverables which can be measured for effectiveness.

Are the roles of the three role players clearly defined and understood?

The roles of each role player are defined in each phase of the framework. The definitions are specific to the phase; therefore the role player knows what is expected of them in each phase. They are also able to understand the roles of other role players in each phase. This approach seeks to make these roles clear for all role players as they become involved in different phases.

8.4 Strengths of the framework

This framework should appeal to the role players that form part of this study. The framework brings together the three role players with a view to assisting them in understanding their respective roles, as well as those of the other role players. It seeks to portray the role players as partners in a process in which there is transparency in terms of how the controls are implemented. Consequently, cooperation and efficiency among the

role players is improved. This is in contrast to the approach where those that implement controls (information security professionals) view those that evaluate the controls (ICT security auditors and regulatory officials) as enemies.

The framework consists of four phases, which include the planning, implementation, support and measurement of information security. Throughout these phases, the process ensures that information security needs are taken into account, thereby providing a rich tool for rolling out an information security programme. Having the role players involved in all the phases ensures that questions are answered closest to the point where they arise. This means that problems are resolved early on in the process thereby resulting in a cost-effective exercise.

The framework produced here is flexible and adaptable, depending on the environment in which it is applied. This flexibility enables its application in different scenarios as well as different industries (e.g. financial and telecommunication industries).

The framework ensures that roles are defined for each role player in each phase. This seeks to eliminate any issues that arise from the misunderstanding of such roles. The use of a RACI model ensures that the person or persons who are responsible, accountable, consulted and informed in each phase are identified. Moreover, the deliverables for each role player are made clear in each phase. The framework also recommends tools that can enable the various role players to deliver what is expected of them.

8.5 Weaknesses of the framework

As was stated in chapter 1, this framework is only applicable to the South African environment. For South African organisations that have presence in other countries the framework may be too restrictive since it does not consider international laws and regulations. Nevertheless, the framework can provide a good starting point even for these organisations.

The framework may also not be suitable for small organisations, in particular those that do not have dedicated information security roles within their structure. It is, however, suitable for large organisations that already have clearly defined roles in the form of information

security professionals, ICT security auditors and the individuals who are responsible for fulfilling regulatory roles (e.g. compliance officers and corporate legal counsels).

This framework has not been tested in a real-world situation, but is based on existing studies and work, as it is based on an interpretive research study. Subsequently, the results are based on the interpretation of the existing literature and may not be objective in the natural sense.

8.6 Future work

The study can be expanded beyond the South African environment. This could be useful for South African organisations that have a presence in other countries.

The framework can also focus on industries other than primary industries (the Financial and Telecommunications sectors) that were the focus of this study. A new angle might be to look at a framework for small organisations which might not necessarily have clearly defined roles for information security.

Finally, as stated in the previous chapters, information security by its very nature is not limited to just the three role players highlighted in this study. There are many other important role players, including the board of directors and the executive management. New research could investigate the way other stakeholders could be involved holistically to ensure alignment in the implementation and evaluation of information security controls.

References

Abdullah, H. 2006, *A risk analysis and risk management methodology for mitigating wireless local area networks (WLANs) Intrusion security risks*, University Of Pretoria.

Africa, S. 2009, , *CSIR ups SA's info-war capabilities* [Homepage of ITWeb], [Online]. Available: http://www.itweb.co.za/index.php?option=com_content&view=article&id=22229:csir-ups-sas-infowar-capabilities&catid=234:security [2009, 06/09].

Alberts, C., Dorofee, A., Stevens, J. & Woody, C. 2003, *Introduction to the OCTAVE® Approach*, Software Engineering Institute, USA.

Alghamdi, A.S. 2010, "A Review of Commercial Related Architecture Frameworks and their Feasibility to C4I System", *European Journal of Scientific Research,* vol. 40, no. 1, pp. 43-49.

Anderson, E.E. & Choobineh, J. 2008, "Enterprise information security strategies", *Computers & Security,* vol. 27, no. 1, pp. 22-29.

Anderson, P.S. 2002, "Critical Infrastructure Protection in the Information Age" in *Networking Knowledge for Information Societies: Institutions and Intervention*, eds. R. Mansell, R. Samarajiva & A. Mahan, Delft University Press, Netherlands, pp. 188-194.

Apani 2006, *Encryption and Segmentation Compensating Controls for PCI DSS Compliance*, Apani Networks, USA.

Ayoub, R. 2011, *The 2011 (ISC)2 Global Information Security Workforce Study*, Frost & Sullivan, USA.

Bailey, A.D. 1979, "A resolution-based approach to the validation of internal control systems", *Annual Conference*ACM, New York.

Banacorsi, S. 2011, , *What is a RACI* [Homepage of 6sixsigma.com], [Online]. Available: http://6sixsigma.com/index.php/Six-Sigma-Articles/RACI-Diagram.html [2011, 10/22].

Basel Committee 2001, *The Basel Capital Accord: an explanatory note*, Bank For International Settlements, Basel.

Brag, R. 2003, *CISSP Certification,* Que, USA.

Business Dictionary 2009, , *Framework*. Available: http://www.businessdictionary.com/definition/framework.html [2009, 09/24].

References

Business Software Alliance 2003, *Information Security Governance: Toward a Framework for Action*, Business Software Alliance, USA.

Butler, A.R. 2006, "Information Systems Security Requirements For Federal GIS Initiatives", *ESRI 2006 Federal User Conference*Washington DC, 2006/02/01.

Carrol, M. 2006, *Information Systems Auditor's Profile*, UNISA.

Cashell, B., Jackson, W., Jickling, M. & Webel, B. 2004, *The Economic Impact of Cyber-Attacks*, Congressional Research Service (CRS), USA.

Chaula, J.S., Yngstrom, L. & Kowalski, S. 2005, "A framework for evaluation of information systems security", *New Knowledge Today*, eds. H.S. Venter, J.H.P. Eloff, L. Labuschagne & M.M. Eloff, Information Security for South Africa - ISSA, Johannesburg, 2005/06/29-2005/07/1, pp. 1.

Chorafas, D.N. 2008, *IT Auditing and Sarbens-Oxley Compliance,* 1st edn, Auerbach, USA.

Comsec 2009, , *Functions of Comsec* [Homepage of Comsec], [Online]. Available: http://www.intelligence.gov.za/Functions/COMSEC.htm [2009, 07/11].

Continental Solutions 2011, , *Tools for RACI Modeling* [Homepage of Continental Solutions], [Online]. Available: http://www.continentalsoftware.com/raci-model/tools/ [2011, 10/22].

COSO 2004a, *Enterprise Risk Management — Integrated Framework (Executive Summary)*, The Committee of Sponsoring Organisations of the Treadway Commission, USA.

COSO 2004b, *Enterprise Risk Management Framework*, The Committee of Sponsoring Organisations of the Treadway Commission, USA.

Courtney, R. 1982, "A Systematic Approach to Data Security", *Computers & Security,* vol. 1, no. 2, pp. 99-112.

Cunningham, B., Dykstra, T., Fuller, E., Hoagberg, M., Little, C., Miles, G. & Schack, T. 2005, *Network Security Evaluation,* Syngress, Waltham.

Da Veiga, A. & Eloff, J.H.P. 2007, "An Information Security Governance Framework", *Information Systems Management,* vol. 24, no. 4, pp. 361-371.

Dagada, R., Eloff, M.M. & Venter, L.M. 2009, "Too Many Laws But Very Little Progress! Is South African Highly Acclaimed Information Security Legislation Redundant?", *ISSA 2009 Conference*, eds. H.S. Venter, M. Coetzee & L. Labuschagne, Information Security South Africa, Johannesburg, 2009/07/6-8.

Daily News Reporter 2008, , *Big question marks about this laptop* [Homepage of IOL News], [Online]. Available: http://www.iol.co.za/news/politics/big-question-marks-about-this-laptop-1.414196 [2009, 11/15].

References

De Wet, P. 2003, , *RIC collateral damage* [Homepage of Brainstorm], [Online]. Available: http://www.brainstormmag.co.za/index.php?option=com_content&view=article&id=1663&Itemid=89 [2009, 05/14].

Deloitte 2011, , *Protection of Personal Information Bill* [Homepage of Deloitte], [Online]. Available: http://www.deloitte.com/view/en_ZA/za/marketsolutions/popi-act/index.htm#POPI [2011, 09/18].

Department Of Communications 2010, *Notice Of Intention To Make South African National Cybersecurity Policy*, Government Notice edn, National, Pretoria.

Dingle, S. 2009, , *Vodacom scam a 'world first'* [Homepage of Fin24], [Online]. Available: http://www.fin24.com/articles/default/display_article.aspx?ArticleId=1518-2386-2432_2538650 [2009, 10/26].

Dlamini, M.T., Eloff, M.M. & Hone, K. 2009, "Towards Requirements Specification For Preparing An Information Security Budget ", *ISSA 2009 Conference*, eds. L. Labuschagne, M. Coetzee & H.S. Venter, Information Security South Africa, South Africa, 2009/07/6-8, pp. 73.

EDP Audit Committee 1995, *Information Systems Security Review Methodology*, International Organisation Of Supreme Audit Institutions.

Eloff, J.H.P. & Eloff, M.M. 2005, "Information Security Architecture", *Computer Fraud & Security,* vol. 11, pp. 10-16.

Emigh, A. 2005, *Online Identity Theft: Phishing Technology, Chokepoints and Countermeasures*, Radix Labs, USA.

Fabian, R. 2007, , *Interdependence of COBIT and ITIL* [Homepage of ISACA], [Online]. Available: http://www.isaca.org/Journal/Past-Issues/2007/Volume-1/Pages/Interdependence-of-COBIT-and-ITIL.aspx [2011, 10/05].

FFIEC 2006, *Information Security,* Federal Financial Institutions Examination Council, USA.

FIC 2004, , *Financial Intelligence Centre Act* [Homepage of Financial Intelligence Centre], [Online]. Available: https://www.fic.gov.za/SiteContent/ContentPage.aspx?id=14 [2009, 06/06].

Fites, P.E., Kratz, M.P.J. & Brebner, A.F. 1988, *Control and Security of Computer Information Systems,* W.H. Freeman & Company, New York.

Fitzgerald, T. & Krause, M. (eds) 2008, *CISO Leadership: Essential Principles for Success*, AUERBACH, USA.

Flowerday, S., Blundell, A.W. & Von Solms, R. 2006, "Continuous Auditing Technologies And Models: A discussion", *Computers & Security,* vol. 25, no. 5, pp. 325-331.

References

Furner, J. & Cheney, K. 2008, *HP Project and Portfolio Management Center Briefing*, Hewlett-Packard Development Company, USA.

GAAS 2010, *, General Accepted Auditing Standards* [Homepage of Americal Institute of CPAs], [Online]. Available: http://www.aicpa.org/Storage/Resources/Standards/DownloadableDocuments/AU-00150.PDF [2010, 06/15].

Garigue, R. & Stefaniu, M. 2003, "Information Security Governance Monitoring", *Information System Security,* vol. 12, no. 4, pp. 36-40.

Gerber, M. & Von Solms, R. 2005, "Management of risk in the information age", *Computers & Security,* vol. 24, pp. 16-30.

Gerber, M. & Von Solms, R. 2001, "From risk analysis to security requirements", *Computers & Security,* vol. 20, pp. 577-584.

Gonzales, C., Senft, S., Gallegos, F. & Manson, D.P. 2004, *Information Technology Control and Audit,* 2nd edn, Auerbach, USA.

Gordon, R. 2003, *, Information Security Threats*. Available: http://www.csis-scrs.gc.ca/prrts/nfrmtn/index-eng.asp [2009, 06/19].

Guldentops, E. 2004, "The IT Dimension of Basel II", *Information Systems Control Journal,* vol. 6.

Hansche, S., Berti, J. & Hare, C. 2004, *OFFICIAL (ISC)2® GUIDE TO THE CISSP® EXAM,* Auerbach, USA.

Harris, S. 2005, *Cissp All-in-one Exam Guide,* 2nd edn, McGraw-Hill Osborne Media, USA.

Hermason, D.R., Hill, M.C. & Ivancevich, M.D. 2000, "Information Technology-Related Activities of Internal Auditors", *Journal of Information Systems,* vol. 14, no. 1, pp. 39-53.

Hoekstra, A. & Conradie, N. 2002, *CobiT, ITIL and ISO17799 How to use them in conjunction*, PriceWaterhouseCoopers (PWC), South Africa.

Hoffman, D. 2007, *Blackjacking: Security Threats to BlackBerry® Devices, PDAs, and Cell Phones in the Enterprise,* Wiley Publishing, USA.

Höne, K. & Eloff, J.H.P. 2002, "What makes an Effective Information Security Policy? ", *Network Security,* vol. 2002, no. 6, pp. 14-16.

Huang, S., Lee, C. & Kao, A. 2006, "Balancing Performance Measures for Information Security Management", *Industrial Management & Data Systems,* vol. 106, no. 2, pp. 242-255.

References

Humphreys, E. 2008, "Information security management standards: Compliance, governance and risk management", *Information Security Technical Report,* vol. 13, no. 4, pp. 247-255.

Idefense 2008, *2009 Cyber Threats and Trends*, Idefense, USA.

IFAC 2011, *, International Auditing and Assurance Standards Board* [Homepage of International Federation Of Accountants], [Online]. Available: http://www.ifac.org/auditing-assurance [2011, 08/21].

IIA 2010, *, Institute of Internal Auditors* [Homepage of Institute of Internal Auditors], [Online]. Available: www.theiia.org [2010, 06/24].

International Chamber Of Commerce 2003, *Information security assurance for executives*, The world business organisation, France.

International Telecommunication Union 2008, *ITU Study on the Financial Aspects of Network Security: Malware and Spam*, International Telecommunication Union, Switzerland.

Internet Service Providers' Association 2007, *, Promotion Of Access To Information Act* [Homepage of Internet Service Providers' Association], [Online]. Available: http://ispa.org.za/regcom/advisories/advisory11.shtml [2009, 06/06].

IRBA 2011, *, **Independent Regulatory Board for Auditors*** [Homepage of Independent Regulatory Board for Auditors], [Online]. Available: www.irba.co.za [2011, 08/22].

ISACA 2011a, *COBIT 5: The Framework,* ISACA, USA.

ISACA 2011b, *Top Business/Technology Issues Survey Results 2011*, ISACA, USA.

ISACA 2009a, *An introduction to the business model for information security*, ISACA, USA.

ISACA 2009b, *The Risk IT Framework,* ISACA, USA.

ISACA 2008a, *CISA Review Manual,* ISACA, Illinois.

ISACA 2008b, *CISM Review Manual 2009,* ISACA, USA.

ISACA 2007, *CISM Review Manual 2007,* ISACA, USA.

ISACA-SA 2012, 11/01/2012-last update*, ISACA South Africa Chapter* [Homepage of ISACA], [Online]. Available: Www.isaca.co.za [2012, 01/11].

ISF 2007, *The Standard of Good Practice for Information Security*, Information Security Forum, London.

ISG-AFRICA 2012, 11/01/2012-last update*, Information Security Group of Africa* [Homepage of ISG], [Online]. Available: Www.isafrica.org [2012, 01/11].

References

ISO/IEC 13335 2004, *Concepts and models for information and communications technology security management,* 1st edn, ISO/IEC, Switzerland.

ISO/IEC 27001 2005, *Information Technology-Security techniques (ISO/IEC 27001:2005),* 1st edn, ISO, Switzerland.

ISO/IEC 27002 2007, *Information technology - Security techniques - Code of practice for information security management,* ISO, Switzerland.

ISSA 2012, 11/01/2012-last update*, Information Security For South Africa* [Homepage of ISSA], [Online]. Available: Www.infosecsa.co.za [2012, 01/11].

IT Governance Institute 2008a, *Aligning CobiT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit*, IT Governance Institute, USA.

IT Governance Institute 2008b, *Cobit Mapping: Mapping of IT v3 With Cobit 4.1,* IT Governance Institute, USA.

IT Governance Institute 2007a, *Cobit 4.1*, IT Governance Institute, USA.

IT Governance Institute 2007b, *IT Controls Objectives for Basel II: The Importance Of Governance And Risk Management For Compliance (Exposure Draft),* IT Governance Institute, USA.

IT Governance Institute 2006, *Information Security Governance: Guidance For Board Of Directors And Executive Management,* 2nd edn, IT Governance Institute, USA.

IT Governance Institute, 2008, *Information Security Governance: Guidance For Information Security Managers,* IT Governance Institute, USA.

ITWeb 2012, 11/01/2012-last update*, ITWeb Security Summit 2012* [Homepage of ITWeb], [Online]. Available: Www.itweb.co.za [2012, 01/11].

Jackson, K.M. & Hruska, J. (eds) 1992, *Computer security reference book*, Butterworth-Heinemann LTD, Oxford.

Jacoby, D. 2010, *, New tool allows script kiddies to build botnets via Twitter!*. Available: http://www.securelist.com/en/blog/2163/New_tool_allows_script_kiddies_to_build_botnets_via_Twitter [2011, 06/29].

Julisch, K., Suter, C., Woitalla, T. & Zimmermann, O. 2011, "Compliance by design- Bridging the chasm between auditors and IT architects", *Computers & Security,* vol. XXX, pp. 1-17.

Karabacak, B. & Sogukpinar, I. 2005, "ISRAM: information security risk analysis method", *Computers & Security,* vol. 24, pp. 147-159.

References

King, M. 2009, *King committe on governance (Draft)*, Institute of directors in Southern Africa, South Africa.

Kritzinger, E. & Smith, E. 2008, "Information security management: An information security retrieval and awareness model for industry", *Computers & Security,* vol. 27, no. 5, pp. 224-231.

Lessing, M.M. 2008, "Best practices show the way to information security maturity", *National Conference on Process Establishment, Assessment and Improvement in Information Technology*Johannesburg, 17-19 September, pp. 1-9.

Liell-Cook, S., Graham, J. & Hill, P. 2009, *, IT Governance Aligned To King III* [Homepage of IT Governance Network], [Online]. Available: http://lgict.org.za/sites/lgict.org.za/files/documents/2009/liell-cock-graham-hill-2009-it-governance-aligned-king-iii.pdf [2010, 12/10].

Liu, E., Yu, J. & Mylopoulos, J. 2002, "Analysing Security Requirements as Relationships Among Strategic Actors", *2nd Symposium on Requirements Engineering for Information Security*CERIAS, Purdue University, North Carolina, October 16.

Loyd, S. 2004, *, Corporate Governance And Information Security* [Homepage of SANS Institute], [Online]. Available: www.sans.org [2011, 06/30].

Mahlong, A. 2009, *, Mpumalanga invites cyber criminals* [Homepage of ITWeb], [Online]. Available: http://www.itweb.co.za/index.php?option=com_content&view=article&id=27156:mpumalanga-invites-cyber-criminals&catid=234 [2009, 11/05].

Manjak, M. 2006, *Social Engineering to Information security*, SANS Institute, USA.

Maphakela, M.R. 2008, *A Model for Legal Compliance in the South African Banking Sector - An Information Security Perspective* -, Masters edn, Nelson Mandela Metropolitan University, Southa Africa.

McKinley, D.T. 2003, *The State of Access to Information in South Africa*, Centre for the Study of Violence and Reconciliation, South Africa.

Mears, L. & Von Solms, R. 2004, "Corporate Information Security Governance: A holistic approach", *ISSA 2004 enabling tomorrow Conference*, eds. H.S. Venter, J.H.P. Eloff, L. Labuschagne & M.M. Eloff, Information Security For South Africa, Johannesburg, 2004/06/30-2004/07/02.

Michalson, L. & Hughes, B. 2005, *Guide to the ECT Act*, Michalson, South Africa.

Mouratidis, H., Giorgini, P. & Manson, G. 2005, "When security meets software engineering: a case of modelling secure information systems", *Information Systems,* vol. 30, pp. 609-629.

References

MS-ISAC 2010,
Security and Privacy on Social Networking Sites, Emergency Management and Response- Information Sharing and Analysis Center, USA.

Nair, M.K. 2009, *, FAQ : What is the difference between Framework and Standard?*. Available: http://madhuottapalam.blogspot.com/2009/10/faq-what-is-difference-between.html [2011, 12/05].

Nanggroe 2011, *, Information Security Roles And Responsibilities*. Available: http://i-data-recovery.com/information-security/information-security-roles-and-responsibilities [2011, 12/05].

National Computing Centre 2005, *IT Governance: Developing a successful governance strategy,* National Computing Centre, Manchester.

Nonaka, T. 2009, *Information Security Framework in Japan*, Japan Information Processing Development Corporation, Japan.

OECD 2004, *OECD Principles of corporate governance*, Organisation for economic co-operation and development, Paris.

Oldsman, E. & Hallberg, K. 2006, *Framework for Evaluating the Impact of Small Enterprise Initiatives*, Nexus Associates Inc., Massachusetts.

Olivia 2011, *, Difference Between Standard and Framework*. Available: http://www.differencebetween.com/difference-between-standard-and-vs-framework/ [2011, 05/12].

Onsett International Corporation 2001, *Information Security Management: Not A Technology Problem*, Onsett International Corporation, Massachusetts.

OregonGov 2009, *, Information security plan* [Homepage of Oregon Government], [Online]. Available: http://oregon.gov/das [2010, 10/10].

Owens, D. 2009, *Application and Website Security 101*, SystemSecurities, USA.

Padayachie, R.L. 2008, *Presentation on Cybersecurity*, Department Of Communication (South Africa), Switzerland.

PCI DSS 2011, *, PCI Security Standards Document* [Homepage of PCI Security Standards Council], [Online]. Available: https://www.pcisecuritystandards.org [2011, 10/05].

Peltier, T.R., Peltier, J. & Blackley, J. 2005, *Information Securiy Fundamentals,* Auerbach, USA.

Pfleeger, P.C. & Pfleeger, S.L. 2002, *Security in Computing,* 3rd edn, Prentice Hall, New Jersey.

References

Pinder, P. 2006, "Preparing Information Security for legal and regulatory compliance (Sarbanes-Oxley and Basel II)", *Information Security Technical Report,* vol. 11, no. 1, pp. 32-38.

Ponemon Institute 2010, *State Of Endpoint Risk*, Ponemon Institute, USA.

Posthumus, S. & Von Solms, R. 2004, "A framework for the governance of information security", *Computers & Security,* vol. 23, pp. 638.

Powner, D.A. 2005, *Critical Infrastructure Protection: Challenges in addressing cybersecurity*, United States Government Accountability Office, USA.

Qayoumi, M.H. & Woody, C. 2005, "Addressing Information Security Risk", *Educause Quarterly,* vol. 28, no. 4, pp. 7-11.

RACI Model 2011, , *Identifying roles and responsibilities: RACI chart* [Homepage of Value Based Management], [Online]. Available: http://www.valuebasedmanagement.net/methods_raci.html [2011, 10/22].

Rees, J., Bandyopadhyay, S. & Spafford, E. 2003, "PFIRES: A Policy Framework for Information Security", *Communications of the ACM,* vol. 46, no. 7, pp. 101-106.

Reitlerlaw 2010, , *Social Networking And The Overlooked Issue Of Security* [Homepage of Reitlerlaw], [Online]. Available: http://www.reitlerlaw.com/Social%20Networking%20and%20the%20Overlooked%20Issue%20of%20Security.pdf [2011, 12/03].

Renton, R. 2009, , *Zurich South Africa discloses loss of data tape with customer information* [Homepage of Zurich South Africa], [Online]. Available: http://www.zurich.co.za/media_relations_release_221009.php [2009, 11/05].

Rose, J. & Norman, C.S. 2008, *Internal Audit Reporting Lines, Fraud Risk Decomposition, and Assessments of Fraud Risk,* The IIA Research Foundation, USA.

Rudd, C. 2004, *An introductory overview of ITIL,* The IT Service Management Forum, United Kingdom.

SA Government 2005, *Auditing Profession Act*, Gazzette edn, South Africa, South Africa.

SABRIC 2009, , *South African Banking Risk Information Centre* [Homepage of South African Banking Risk Information Centre], [Online]. Available: www.sabric.co.za [2009, 06/06].

SABSA 2011, , *SABSA Overview* [Homepage of SABSA], [Online]. Available: http://www.sabsa.org/the-sabsa-method/sabsa-overview.aspx [2011, 11/11].

SAFPS 2009, , ***Frontrunners in the fight against fraud*** [Homepage of South African Fraud Prevention Service], [Online]. Available: http://shamwari.safps.org.za/shamwariweb/AboutUs.aspx [2009, 06/06].

References

Sagar, A. 2005, *Various Types of Attacks and Countermeasures*, Indian Computer Emergency Response Team.

SAHRC 2009, *, Access To Information* [Homepage of South African Human Rights Commission], [Online]. Available: http://www.sahrc.org.za/sahrc_cms/publish/cat_index_70.shtml [2009, 06/06].

Saleh, M.S. & Alfantookh, A. 2011, "A new comprehensive framework for enterprise information security risk management", *Applied Computing and Informatics,* vol. 9, pp. 107-118.

SAPA 2009, *, Cybercrime syndicate swindles govt out of R199m* [Homepage of Mail & Guardian online], [Online]. Available: http://mg.co.za/article/2008-06-10-cybercrime-syndicate-swindles-govt-out-of-r199m [2009, 10/26].

Sherwood, J., Clark, A. & Lynas, D. 2009, *Enterprise Security Architecture*, SABSA, Sussex, USA.

SoftScout 2011, *, CORA® Cost-of-Risk Analysis by International Security Technology, Inc.* [Homepage of SoftScout], [Online]. Available: http://www.softscout.com/software/Project-and-Business-Management/Risk-Management/CORA--Cost-of-Risk-Analysis.html [2011, 12/05].

Spremic, M. 2011, "Standards and Frameworks for Information System Security Auditing and Assurance", *Proceedings of the World Congress on Engineering 2011*, eds. S.I. Ao, C. Douglas, W.S. Grundfest & J. Burgstone, International Association of Engineers (IAENG), UK, 2011/07/6-8.

Stavrou, A. 2002, *Mission Impossible: E-Security In South Africa's Commercial And Financial Sectors,* Institute for Security Studies, South Africa.

Sundt, C. 2006, "Information Security and the Law", *Information Security Technical Report,* vol. 11, no. 1, pp. 2-9.

Symantec 2011, *, Norton Study Calculates Cost of Global Cybercrime: $114 Billion Annually*. Available: http://www.symantec.com/about/news/release/article.jsp?prid=20110907_02 [2011, 08/13].

Symantec 2008, *Financial Services Information Security and IT Risk Management*, Symantec, USA.

The Open Group 2011, *Open Information Security Management Maturity Model (O-ISM3),* The Open Group, UK.

ThesisTown 2009, *, Analyzing inconsistency in evolving security requirements* [Homepage of ThesisTown], [Online]. Available: http://thesistown.com/data/proposal.pdf [2010, 09/30].

References

Tipton, H.F. & Krause, M. (eds) 2004, *Information Security Management Handbook*, 5th edn, AUERBACH, USA.

Trcek, D. 2003, "An integral framework for information systems security management", *Computers & Security,* vol. 22, no. 4, pp. 337-360.

Trinckes, J.J. 2009, *The Executive MBA in Information Security,* 1st edn, CRC Press, USA.

Tucci, L. 2009, *, How CISOs can leverage the internal audit process* [Homepage of SearchCompliance.com], [Online]. Available: http://searchcompliance.techtarget.com/news/1362909/How-CISOs-can-leverage-the-internal-audit-process [2010, 09/09].

Ula, M., Ismail, Z. & Sidek, Z.M. 2011, "A Framework for the Governance of Information Security in Banking System", *Journal of Information Assurance & Cybersecurity,* vol. 2011 (2011).

Vinh, T.V. & Grewal, D.S. 2005, "Critical success factors of effective security management: a survey of Vietnamese maritime transport service providers", *International Association of Maritime Universities (IAMU) 6th Annual General Assembly and Conference*, ed. D. Nielsen, World Maritime University, Sweden, 2005/10/24-26, pp. 87-96.

Von Solms, B. 2006, "Information Security – The Fourth Wave", *Computers & Security,* vol. 25, pp. 165-168.

Von Solms, B. 2005, "Information Security governance: COBIT or ISO 17799 or both?", *Computers & Security,* vol. 24, pp. 99-104.

Von Solms, B. 2001, "Information Security - A Multidimensional Discipline", *Computers & Security,* vol. 20, no. 6, pp. 504-508.

Von Solms, B. & Von Solms, R. 2004, "The 10 deadly sins of information security management", *Computers & Security,* vol. 23, no. 5, pp. 371-376.

Von Solms, R. & Von Solms, S.H. 2006a, "Information Security Governance: A model based on the Direct–Control Cycle", *Computers & Security,* vol. 25, pp. 408-412.

Von Solms, R. & Von Solms, S.H. 2006b, "Information security governance: Due care", *Computers & Security,* vol. 25, pp. 494-497.

Vorster, A. & Labuschagne, L. 2005, "A Framework for Comparing Different Information Security Risk Analysis Methodologies", *New Knowledge Today*, eds. H.S. Venter, J.H.P. Eloff, L. Labuschagne & M.M. Eloff, Information Security For South Africa - ISSA, Johannesburg, 2005/06/29-2005/07/01.

Warner, T. & Harris, S. 2010, *, A Conversation with Shon Harris on IT Security*. Available: http://www.pearsonitcertification.com/articles/article.aspx?p=1646450 [2011, 06/219].

References

Weil, S. 2010, , *How ITIL Can Improve Information Security* [Homepage of Symantec], [Online]. Available: http://www.symantec.com/connect/articles/how-itil-can-improve-information-security [2011, 10/09].

Williams, P. 2007, "Executive and board roles in information security", *Network Security,* , no. 8, pp. 11-14.

Wilson, C. 2008, *Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress*, Congressional Research Service, USA.

Wright, C. 2008, *The IT regulatory and standards compliance handbook: How to survive an information systems audit and assessments,* Syngress, Waltham.

Wybourne, M.N., Austin, M.F. & Palmer, C.C. 2009, *National Cyber Security: Research and Development Challenges*, Institute for Information Infrastructure Protection (I3P), USA.

Zachman, J.A. 2011, *The Zachman Framework for Enterprise Architecture: The Enterprise Ontology*, Zachman International, USA.

Zimmermann, O. 2009, *An Architectural Decision Modelling Framework for Service-Oriented Architecture Design*, University of Stuttgar.

UNISA university of south africa

STUDENT NUMBER 4599 124 3

2 BOUND **COPIES OF**

DISSERTATION/THESIS

RECEIVED FROM BASANI M

FOR THE DEGREE MSC

DATE 6.12.2012

SIGNATURE

University of South Africa
Preller Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za