A FRAMEWORK FOR INFORMATION SECURITY GOVERNANCE IN SMMEs

by

Jacques Jacobus Coertze

2012

A FRAMEWORK FOR INFORMATION SECURITY GOVERNANCE IN SMMEs

by

Jacques Jacobus Coertze

Dissertation

submitted in fulfilment

of the requirements

for the degree

Magister Technologiae

in

Information Technology

in the

Faculty of Engineering, the Built Environment and Information Technology

at the

Nelson Mandela Metropolitan University

Promoter: Prof. Rossouw von Solms

February 2013

Declaration

I, Jacques Jacobus Coertze, hereby declare that

- the work in this dissertation is my own work
- all sources used or referred to have been documented and recognised
- this dissertation has not previously been submitted in full or partial fulfilment of the requirements for an equivalent or higher qualification at any other recognised educational institute.

JJCoertze

Jacques Jacobus Coertze

Abstract

It has been found that many small, medium and micro-sized enterprises (SMMEs) do not comply with sound information security governance principles, specifically the principles involved in drafting information security policies and monitoring compliance, mainly as a result of restricted resources and expertise. Research suggests that this problem occurs worldwide and that the impact it has on SMMEs is great. The problem is further compounded by the fact that, in our modern-day information technology environment, many larger organisations are providing SMMEs with access to their networks. This results not only in SMMEs being exposed to security risks, but the larger organisations as well. In previous research an information security management framework and toolbox was developed to assist SMMEs in drafting information security policies. Although this research was of some help to SMMEs, further research has shown that an even greater problem exists with the governance of information security as a result of the advancements that have been identified in information security literature. The aim of this dissertation is therefore to establish an information security governance framework that requires minimal effort and little expertise to alleviate governance problems. It is believed that such a framework would be useful for SMMEs and would result in the improved implementation of information security governance.

Keywords: automation; information security; corporate governance; enterprise security; information technology governance; information security governance; managing information security; security policy and procedures; methodologies for securing small/medium size enterprises

Acknowledgements

I would like to thank my supervisor, Professor Rossouw von Solms, whose knowledge, guidance, support and patience have played a major role in the completion of this dissertation. I would also like to thank the National Research Foundation for the funding that they provided. In addition, I would like to thank my family for their constant support and encouragement.

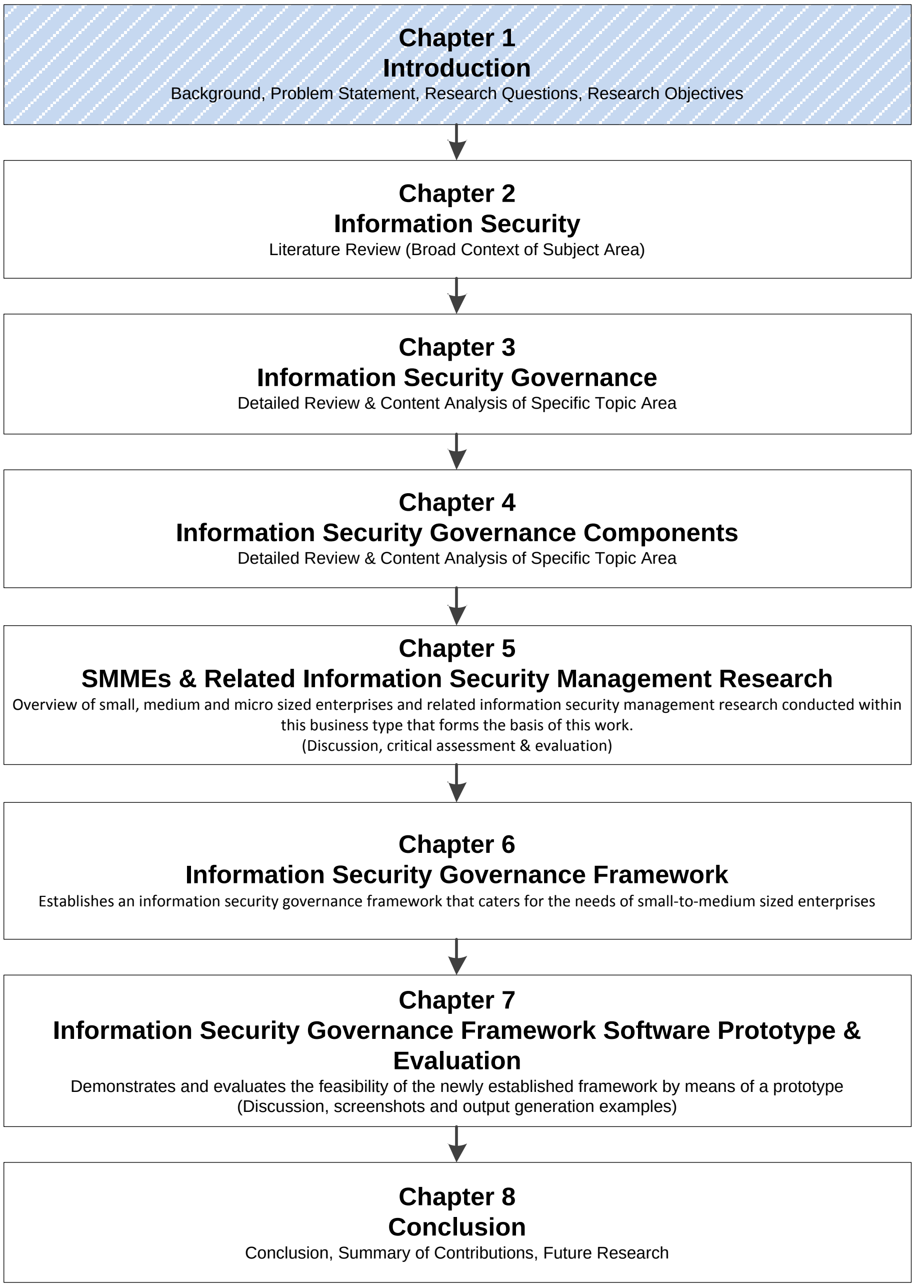
Table of Contents

List of Tables

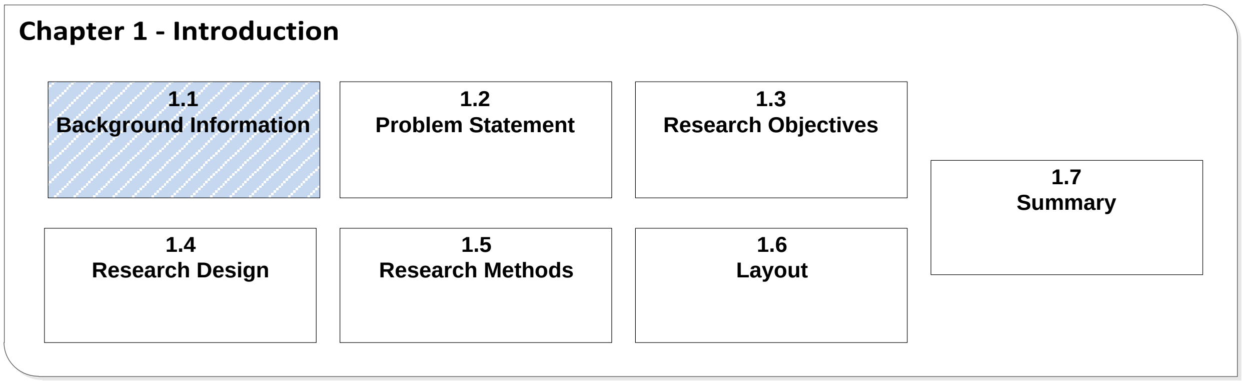
List of Figures

Chapter 1: Introduction

"The emergence and evolution of the internet (information), e-commerce, on-line trading and electronic communication have enabled companies to conduct business electronically and perform transactions instantly. These developments bring about significant risks and should (therefore) be well governed and controlled" (Institute of Directors in Southern Africa, 2009a, p. 16)


Chapter 1
Introduction
Background, Problem Statement, Research Questions, Research Objectives
Chapter 2
Information Security
Literature Review (Broad Context of Subject Area)
Chapter 3
Information Security Governance
Detailed Review & Content Analysis of Specific Topic Area
Chapter 4
Information Security Governance Components
Detailed Review & Content Analysis of Specific Topic Area
Chapter 5
SMMEs & Related Information Security Management Research
Overview of small, medium and micro sized enterprises and related information security management research conducted within this business type that forms the basis of this work.
(Discussion, critical assessment & evaluation)
Chapter 6
Information Security Governance Framework
Establishes an information security governance framework that caters for the needs of small-to-medium sized enterprises
Chapter 7
Information Security Governance Framework Software Prototype & Evaluation
Demonstrates and evaluates the feasibility of the newly established framework by means of a prototype
(Discussion, screenshots and output generation examples)
Chapter 8
Conclusion
Conclusion, Summary of Contributions, Future Research

1.1 Background Information



The role that information plays and its importance in business continue to be crucial in the ever-evolving business environment of today; accordingly, the protection, and governance of information should not be taken lightly. This section explains what information security and information security governance is and then goes on to define information security policies and compliance monitoring in relation to the governance of information security. This section concludes by identifying the difficulties and challenges experienced by small, medium and micro-sized enterprises (SMMEs) in this regard.

1.1.1 Information Security and Governance

1.1 Background Information
1.1.1 Information Security & Governance
1.1.2 Policies & Compliance Monitoring
1.1.3 Previous Research Conducted

Information is a critical business asset for any organisation, irrespective of its size (Von Solms, 1998). It has thus become the operational lifeblood of most organisations (R. Von Solms & Von Solms, 2006a). The many benefits that organisations reap from information include providing them with a competitive edge, allowing for financial prosperity and providing real-time reporting (Posthumus, Von Solms, & King, 2010). In this day and age, such benefits do not simply happen on their own, but require technology as an enabler. Information technology (IT) is such an enabler and is used to store, process and transmit critical business information.

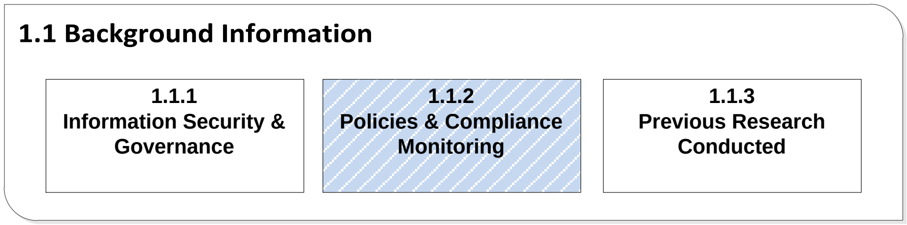
IT is essential for managing the information and knowledge required in the daily operations of an organisation. It has, thus, become an integral part of most businesses and is vital to their growth (IT Governance Institute, 2003, p. 7). Such growth comes at a price, however, as today many security threats exist that threaten both IT and information per se (S. Von Solms & Von Solms, 2008, p. iv). Consequently, both IT and information have to be protected using proper information security measures that will ensure continued growth and derived benefit (ISO/IEC 27002, 2005, p. viii).

Information security pertains to the protection of the confidentiality, integrity and availability of information (ISO/IEC 27002, 2005, p. 1) and is generally attained through a process called information security management. Such protection must be properly governed (Posthumus et al., 2010) through a process termed "information security governance", which is a subcomponent of corporate governance (S. Von Solms & Von Solms, 2008, p. 17).

Information security governance, as a component of corporate governance (see Institute of Directors in Southern Africa, 2009a), is the responsibility of the organisation's executive management (Coertze, Van Niekerk, & Von Solms, 2011; Posthumus et al., 2010; R. Von Solms & Von Solms, 2006a). Accordingly, executive management is required to both direct and control information security according to sound corporate governance principles (Du Plessis, Hargovan, & Bagaric, 2011, p. 3; Institute of Directors in Southern Africa, 2009a, pp. 86–87; R. Von Solms & Von Solms, 2006a). Many guiding documents, in the form of best practices and standards, exist to assist executive management in these tasks (Institute of Directors in Southern Africa, 2009a; ISO/IEC 27002, 2005; IT Governance Institute, 2007).

Information security, in particular the governance thereof, has been discussed as the area of study for this dissertation. It is now important to identify the focus of this dissertation by providing a brief overview of the guiding documentation on information security. A special emphasis will be placed on the importance of policies and compliance with them. It will, as a result, become evident that a problem exists pertaining to SMMEs in the area of information security governance, specifically with regard to the drafting of policies and ensuring adequate compliance en route to sound governance.

1.1.2 Policies and Compliance Monitoring


1.1 Background Information
1.1.1
Information Security & Governance
1.1.2
Policies & Compliance Monitoring
1.1.3
Previous Research Conducted

Information security governance and its importance in the business environment have been discussed as the area for study. In addition, it has been highlighted that there is guiding documentation for the successful implementation of information security governance in organisations. This section indicates the focus of this dissertation by discussing some of the core documentation in the field of information security governance and the importance of directing and controlling information security properly.

There are many guiding documents that assist organisations in establishing proper information security governance and management. The international standard ISO/IEC 27002 (2005) focuses specifically on information security management and is supported by the certification standard ISO/IEC 27001 (2005). In support of these two standards, much guiding documentation has been written to provide detail on both corporate and information security governance. These include CoBiT 4.1 (IT Governance Institute, 2007), CoBiT 5 (ISACA, 2012a) and the King III Report (Institute of Directors in Southern Africa, 2009a).

These documents all show that the effective establishment of policies is crucial to information security governance. The documents also mention that the enforcement and compliance monitoring of policies are essential components of governance.

The drafting of an information security policy is usually general practice in organisations and has the purpose of guiding and controlling the actions and behaviour of employees (Knapp, Franklin Morris Jr., Marshall, & Byrd, 2009). The objective of such a policy is to provide managerial direction and support for information security in line with the business's requirements and the applicable laws and regulations (Knapp et al., 2009). Managerial direction and support for such policy is typically captured in the form of instructions and actions, which obviously differ from one business to the next (Yildirim, Akalp, Aytac, & Bayram, 2010). These instructions and actions are usually documented in terms of general statements, including the rules and applications regulating the liability of employees, the aims and goals of security control tools and their proper management. Such a policy should also explain the protection and distribution of business information entities and the protection of important functions (Yildirim et al., 2010). As previously mentioned, policies alone have no value unless the organisation is able to monitor and enforce them.

According to R. Von Solms and Von Solms (2006), corporate governance, and indeed all types of governance, comprise three clear actions, namely, direct, execute and control. A "direct" action predominantly involves, as stipulated above, establishing, and implementing policies in an organisation. The "execute" action, on the other hand, involves the day-to-day application of the policies and the procedures related to them. Finally, the "control" action involves enforcing and monitoring these policies.

As highlighted previously, measurability should be central to all policies produced during the direct action. It is of no use to include a certain clause in an information security policy document if one cannot measure it (Upfold & Sewry, 2005; R. Von Solms & Von Solms, 2006a; S. Von Solms & Von Solms, 2008, p. 44; Yildirim et al., 2010). Any statements that cannot be measured for compliance should therefore rather be excluded from policies (R. Von Solms & Von Solms, 2006a); the reason being that information security policies generate value only when compliance and measurability can be tested. Information security policies will typically include statements with supporting compliance clauses that indicate how compliance checking and measurability will be performed and evaluated (S. Von Solms & Von Solms, 2008, p. 75). These compliance clauses play a vital role in compliance monitoring.

Compliance monitoring and enforcement are vital in ensuring that a secure operational environment is maintained within an organisation. Simply drafting a policy and distributing it among the employees of a business does not automatically result in such a policy being accepted and complied with (R. Von Solms & Von Solms, 2006a). For this to happen the business has to perform frequent, if not real-time, monitoring and enforcement (R. Von Solms & Von Solms, 2004). It should be noted that SMMEs regard drafting policies and monitoring compliance with such policies as difficult tasks (Yildirim et al., 2010). It is therefore vital that SMMEs be assisted in this regard so that secure operational environments are assured.

SMMEs are generally born out of entrepreneurial passion and limited funding, which means that information security governance is often not implemented properly (Upfold & Sewry, 2005). Improper information security governance may result in these enterprises experiencing severe financial problems or it can even lead to business failure (Upfold & Sewry, 2005). To avoid business failure, proper governance practices suggest that SMMEs, like all modern organisations, should both direct and control information security (Institute of Directors in Southern Africa, 2009a, p. 20). This is not happening, however, since shareholders and/or executive management are not being held accountable or in some cases they are not even appointed (Upfold & Sewry, 2005). The result is that whereas large organisations will spend money on information security, SMMEs often lack the resources needed to do so (Tawileh, Hilton, & McIntosh, 2007). SMMEs typically operate with very tight budgets, limited manpower and many competing needs (Gupta & Hammond, 2005; Tawileh et al., 2007; Upfold & Sewry, 2005; Yildirim et al., 2010). This lack of resources often results in corners being cut when it comes to the implementation of proper information security governance (Gupta & Hammond, 2005).

It is ironic that a lack of adequate information security governance in SMMEs exists at a time when IT is playing an ever-increasing role in business processes and business connectivity to public networks is increasing (Upfold & Sewry, 2005). Moreover, SMMEs are becoming contractors to and partners in larger organisations and, as a result, are gaining access to public networks (Upfold & Sewry, 2005).

SMMEs typically have limited resources (Upfold & Sewry, 2005; Yildirim et al., 2010), such as finances and expertise, resulting in difficulties being experienced when attempting to draft policies and ensure compliance with them (Vermeulen & Von Solms, 2002). Consequently, owing to a lack of policies and compliance, many enterprises are at risk of severe information security breaches (Yildirim et al., 2010). This dissertation aims to address this issue by focusing on the field of information security and, in particular, on information security governance, mainly within the context of SMMEs.

From the above statements it can be argued that SMMEs have difficulty in implementing sound information security governance. As has been indicated that adequate guidelines exist, pertaining to information security governance, and that a theme of policy drafting and compliance monitoring is ever-present therein. The principles of policy drafting and compliance monitoring within information security governance implementation are vital, but research shows that these principles are often not present in SMMEs (Gupta & Hammond, 2005; Tawileh et al., 2007; Upfold & Sewry, 2005; Yildirim et al., 2010). The focus of this dissertation is thus to contribute to effective information security governance, specifically focusing on the drafting of policies and compliance monitoring in SMMEs. Research that has been completed with respect to solving this problem will be discussed next. This will be followed by a justification for the research undertaken.

1.1.3 Previous Research Conducted

1.1 Background Information
1.1.1 Information Security & Governance
1.1.2 Policies & Compliance Monitoring
1.1.3 Previous Research Conducted

The directing and controlling of information security governance, that is, policy drafting and compliance monitoring, are vital in ensuring a secure operational environment. Previous research conducted to assist SMMEs with the activities of information security management and governance is outlined below.

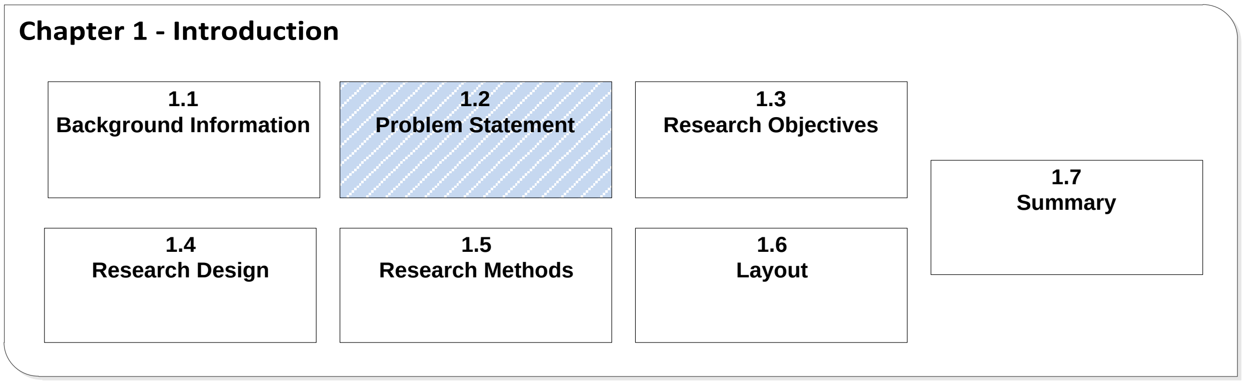
Upfold and Sewry (2005) conducted research in the Eastern Cape and found that the level of information security awareness and practice in SMMEs was inadequate, owing to the fact that SMMEs generally had limited resources and expertise. The research concluded that although there are many frameworks for information security governance, these do not take into account the constraints placed on SMMEs. Similar research was conducted in Burma (Turkey) (Yildirim et al., 2010), the results of which corresponded with those of Upfold and Sewry; that is, up to 58% of respondents found their information security governance and policies to be ineffective.

The findings of the research discussed above are also supported by Gupta and Hammond (2005), who found that many SMMEs were so preoccupied with day-to-day operations that they neglected information security governance in general. Their research also showed that in many cases information security governance was only seen as necessary once the business had faced a serious information security breach. Consequently, it was found that only 48% of their respondents had some form of written information security policy. The findings of inadequate policy drafting and potential lack of compliance monitoring were supported by Upfold and Sewry (2005), Burns, Davies and Davies (2006) and Yildirim et al. (2010).

A previous research project conducted in this field of study resulted in a framework to assist SMMEs with the process of drafting information security policies (Vermeulen & Von Solms, 2002). This framework was successfully implemented in a working prototype, called the Information Security Management Toolbox (ISMTB) (Hoppe, Van Niekerk, & Von Solms, 2002).

In 2011, Coertze et al. (2011) found that the previously discussed framework and associated prototype had become outdated and no longer catered for modern-day information security governance. The main reason for this was that neither the framework nor the prototype provided for the compliance monitoring and strategic-level management involvement that is core to sound information security governance.

1.2 Problem Statement



A business problem has therefore been identified pertaining to the sound implementation of information security governance in SMMEs. The aim of this section is to provide a clear statement about the problem that is addressed in this dissertation.

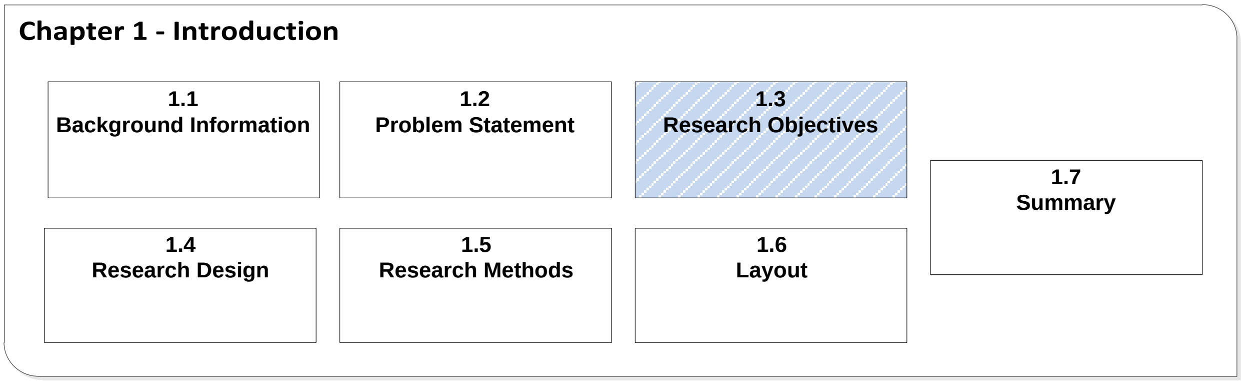
The problem at hand may be articulated as the fact that, owing to a lack of expertise and resources, many SMMEs experience difficulties with drafting information security policies and ensuring their compliance by employees and therefore find it difficult to implement information security governance successfully.

The problem statement can thus be defined as the following:

> Many SMMEs do not comply with sound information security governance principles, specifically those of information security policy drafting and compliance monitoring; this is mainly as a result of limited resources and expertise.

The problem statement that this dissertation addresses and attempts to resolve has now been defined. The research objectives that have been formulated to address this problem statement will be discussed in the next section.

1.3 Research Objectives



The primary objective of this dissertation is to develop a framework, supported by a fully functional software prototype, to assist in governing information security with minimal effort and expertise in the SMME sector. This framework should use concepts and principles that are applicable and usable by SMMEs.

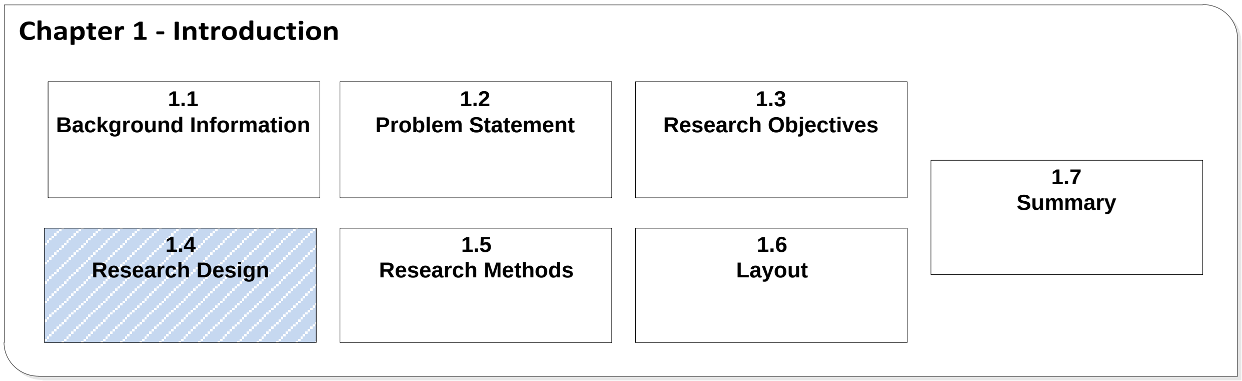
This framework will be based on an existing information security management framework that was developed by Vermeulen and Von Solms (2002), as well as pertinent literature on information security governance principles and the unique characteristics of SMMEs. The framework should also provide guidelines for its realisation and implementation as a software application or prototype.

Secondary objectives include the following:

- to determine the current state of information security governance in SMMEs
- to determine the principles that should be exhibited by a framework for assisting SMMEs in the sound implementation of information security governance
- to establish an information security governance framework for implementing suitable information security governance in an organisation
- to validate the framework by using a software prototype implementation to assist SMMEs in their information security governance implementations.

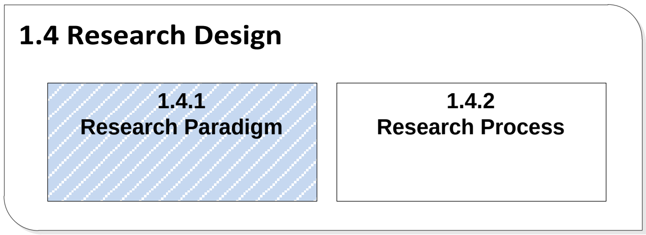
As previously stated, this dissertation addresses a real-world business problem; that is, that many SMMEs do not implement or comply with sound information security governance principles. A solution to this business problem will be provided by means of the objectives stated above.

1.4 Research Design



The problem statement for this dissertation is defined in the form of a specific real-world business problem experienced by SMMEs today. The objective of this dissertation is to find a solution to this business problem. The research design that will ensure that the research objectives do indeed present a solution to this problem situation is described in the following section, which details the research paradigm, process and methods.

1.4.1 Research Paradigm



The main objective of this dissertation is to find a solution to problems experienced by SMMEs when implementing information security governance. This solution will take the form of a framework. It can, therefore, be argued that according to Peffers et al. (2007), and supported by Hevner et al. (2004), the paradigm of design science is ideally suited to this dissertation.

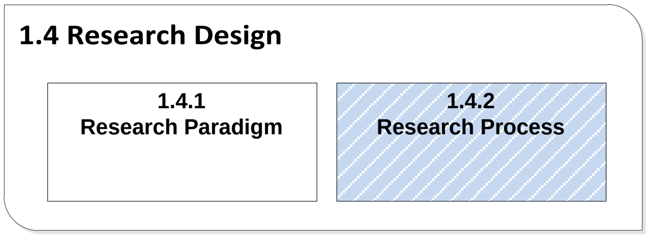
Peffers, Tuunanen, Rothenberger and Chatterjee (2007, p. 48) maintain that “design science attempts to create things that serve human purpose”. They continue by stating that design science concerns itself with creating artefacts that solve organisational (real-world) problems.

It should also be noted that design science follows a specific research process, where key steps lead a researcher's actions (Hevner et al., 2004; Peffers et al., 2006). What differentiate design science from other paradigms is the key steps within the research process, that is, those of artefact design/creation and feasibility evaluation. Therefore, the design science paradigm comprises research performed by creation, or design.

This dissertation, based on the argument above, makes use of the design science paradigm as stipulated by Peffers et al. (2007). It should be noted that Peffers et al. combines the viewpoints of various authors on the design science paradigm in order to create a single definition that should eliminate some of these authors’ contradictions.

In summary, design science is applicable to this dissertation since a definitive business or organisational problem in SMMEs is being addressed and a solution in the form of a framework is designed. To ensure that rigour is maintained throughout this dissertation, a specific, well-defined research process is followed, which is outlined below.

1.4.2 Research Process



Peffers et al. (2007) established a methodology and conceptual model for the design science paradigm. The research process followed the guidelines for the design science paradigm offered by various authors, including Hevner et al. (2004) and March and Smith (1995). Owing to the fact that these authors' guidelines are very similar, the research process is applicable to many different cases. The author of this dissertation therefore makes use of the research process presented by Peffers et al. (2006).

The design science research process (DSRP) model (Peffers et al., 2006) includes six general steps:

1. Problem identification and motivation
2. Objectives for a solution
3. Design and development
4. Demonstration
5. Evaluation
6. Communication.

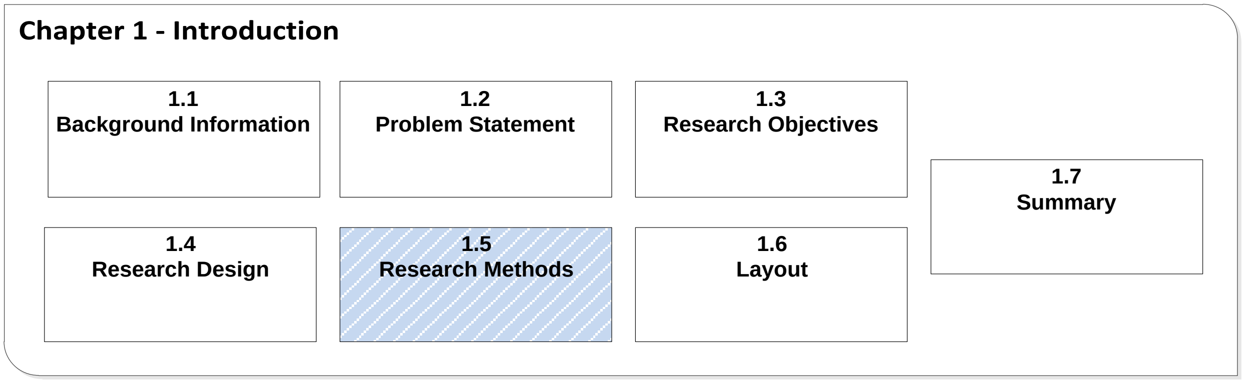
In this dissertation, the steps are implemented as follows:

1. Literature is consulted on information security governance and SMMEs. The aim is to identify and substantiate the existence of a business problem, specifically the improper implementation of information security governance in SMMEs. Additionally, an attempt is made to provide substantial support for the importance of solving the business problem.
2. Literature is consulted to determine the principles that must be exhibited by a solution to the business problem, in the form of a framework to assist in the sound implementation of information security governance in SMMEs. Specific attention is paid to the principles of compliance monitoring and strategic-level management involvement with regard to information security governance.
3. An information security governance framework is developed and proposed for implementing information security governance in an organisation. The framework should be easy to apply and should make use of limited specialised resources, specifically in the SMME environment.
4. The solution, in the form of the framework, is implemented as a working software prototype, based on the existing ISMTB prototype which should be feasible for solving the business problem.

5. The framework and prototype are evaluated to determine the effectiveness and efficiency with which they solve the business problem. The evaluation method used for this purpose entails a focus-group study performed in an industry setting.
6. The framework and resultant findings are subsequently communicated in this dissertation and evidence from two academic peer-reviewed conference papers is provided.

To conclude, Peffers et al. (2006) established a research process that could be used within a design science paradigm. This research process is used by this dissertation, since it is confirmed by various authors on the design science paradigm.

1.5 Research Methods



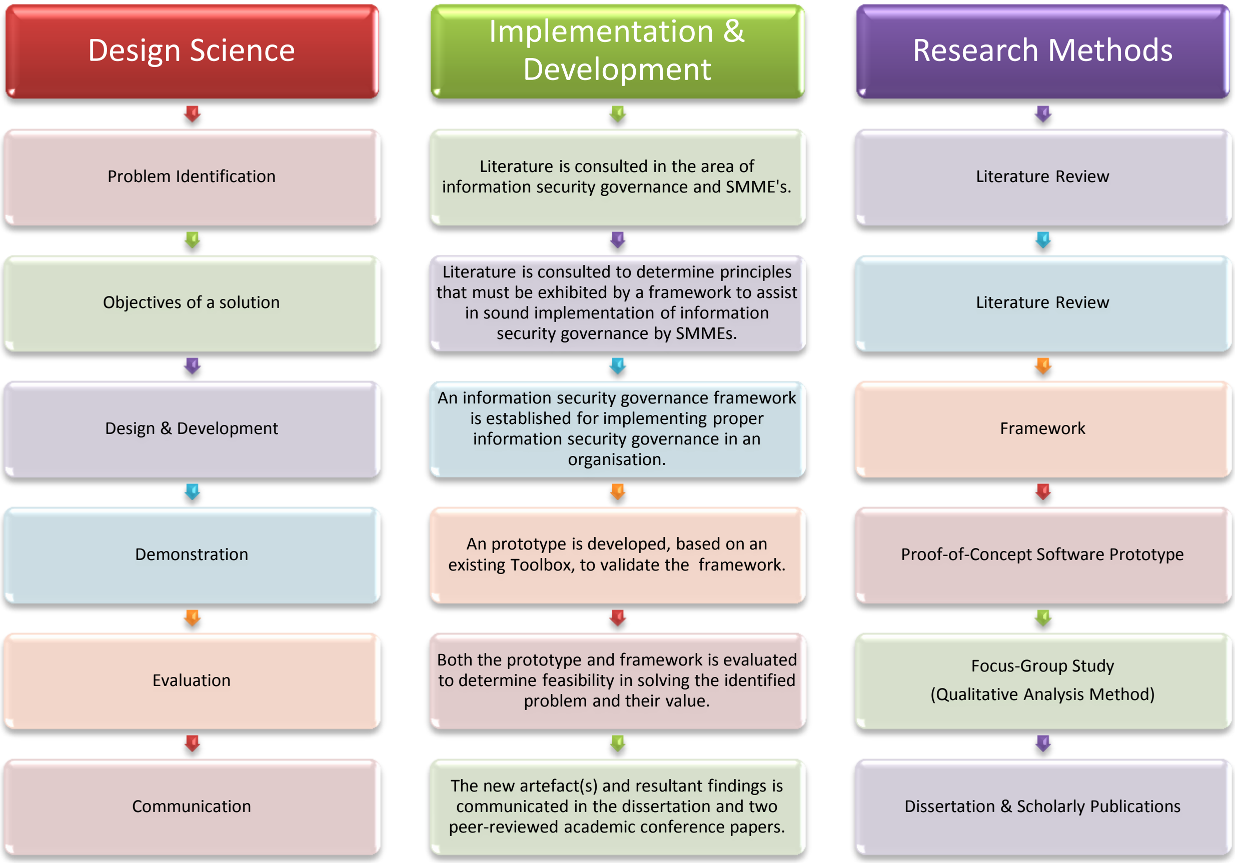
It is important to note that the solution to the business problem presented as the objective of this dissertation takes the form of an artefact – a framework which is depicted using modelling techniques.

According to *The American Heritage Dictionary of the English Language* (2011), a framework is “a set of assumptions, concepts, values, and practices that constitutes a way of viewing reality or a fundamental structure”.

Each research step in the process listed above is approached using an appropriate research method(s). The applicable method(s) for each step is presented below:

1. A literature review of information security governance and SMMEs
2. A literature review of the governance principles required for information security governance
3. A framework
4. An proof-of-concept software prototype
5. A focus-group study conducted in an industry setting (qualitative analysis method)
6. Dissertation and scholarly publications

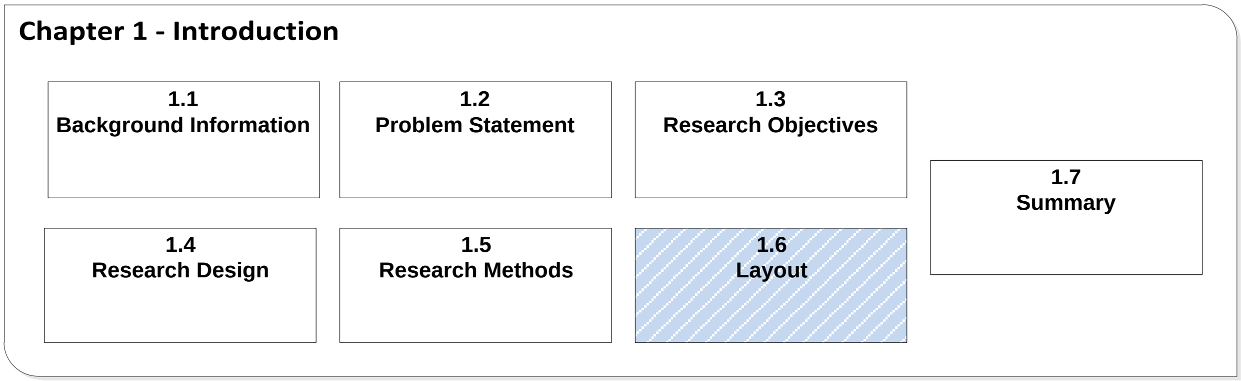
In summary, this dissertation is conducted according to the design science paradigm. In support of the paradigm, a research process, as described by Peffers et al. (2006) is used. A diagram depicting this process, related implementation details and related research methods appears in Figure 1.1.



Design Science	Implementation & Development	Research Methods
Problem Identification	Literature is consulted in the area of information security governance and SMME's.	Literature Review
Objectives of a solution	Literature is consulted to determine principles that must be exhibited by a framework to assist in sound implementation of information security governance by SMMEs.	Literature Review
Design & Development	An information security governance framework is established for implementing proper information security governance in an organisation.	Framework
Demonstration	An prototype is developed, based on an existing Toolbox, to validate the framework.	Proof-of-Concept Software Prototype
Evaluation	Both the prototype and framework is evaluated to determine feasibility in solving the identified problem and their value.	Focus-Group Study (Qualitative Analysis Method)
Communication	The new artefact(s) and resultant findings is communicated in the dissertation and two peer-reviewed academic conference papers.	Dissertation & Scholarly Publications

Figure 1.1 – Research process

1.6 Layout



This dissertation consists of eight chapters. These chapters are briefly described below. Figure 1.2 illustrates the layout of the chapters.

Chapter 1 – Introduction

This chapter introduces the research by describing the research area, the research problem and the objectives that will be met by this work.

Chapter 2 – Information Security

This chapter briefly describes information security. It highlights the importance of information in modern business, demonstrates that risks exist that threaten the organisation's information and describes how such risks can be mitigated by means of information security practices. It concludes by mentioning that information security must be properly managed and governed.

Chapter 3 – Information Security Governance

This chapter briefly describes corporate-, information technology- and information security governance. It highlights how important it is that information security be escalated and addressed as a governance issue and how this should take place.

Chapter 4 – Information Security Governance Components

In this chapter the components necessary for the implementation of information security governance are investigated in more detail. The chapter particularly highlights the necessity for and use of these components.

Chapter 5 – Small, Medium and Micro-sized Enterprises and Related Information Security Management Research

This chapter briefly introduces the reader to SMMEs. Firstly, the characteristics of this business type are provided, its importance to the world economy is highlighted and the problems such businesses face in terms of information security governance implementation are mentioned. Subsequently, the research that has been conducted to assist this business type in resolving the problems mentioned is investigated.

Chapter 6 – Information Security Governance Framework

In this chapter the reader is briefly introduced to the information security governance framework that represents the solution to the problem this work investigated. Firstly, the characteristics of a successful information security governance framework are established and, subsequently, the established framework is depicted and discussed using a conceptual model.

Chapter 7 – Information Security Governance Framework Software Prototype and Evaluation

This chapter briefly describes a software prototype that has been developed to demonstrate the information security governance framework. Further, by means of this prototype, the findings of an evaluation performed to ascertain the feasibility of the information security governance framework are discussed.

Chapter 8 – Conclusion

This chapter draws conclusions based on the research presented in the preceding chapters.

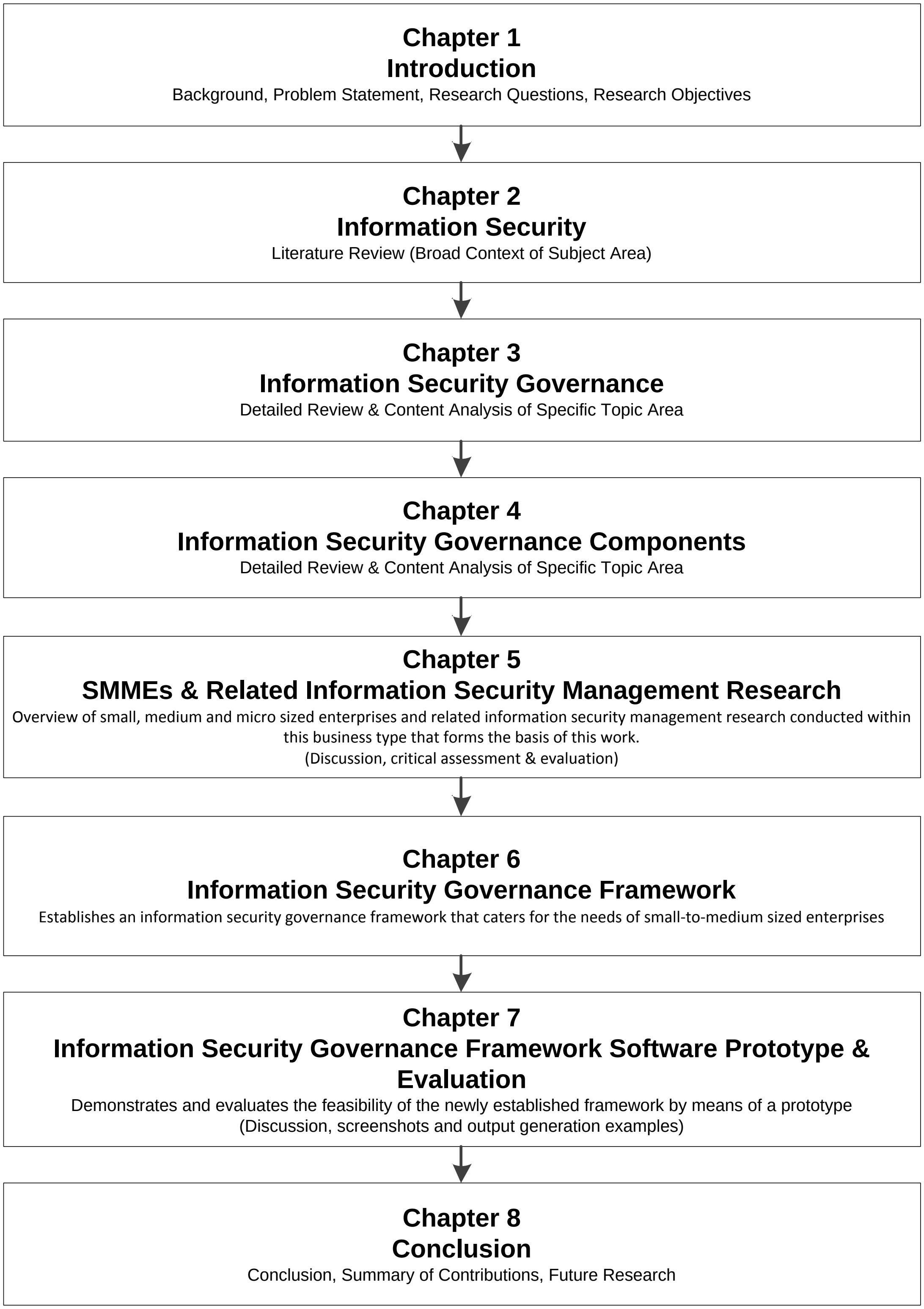
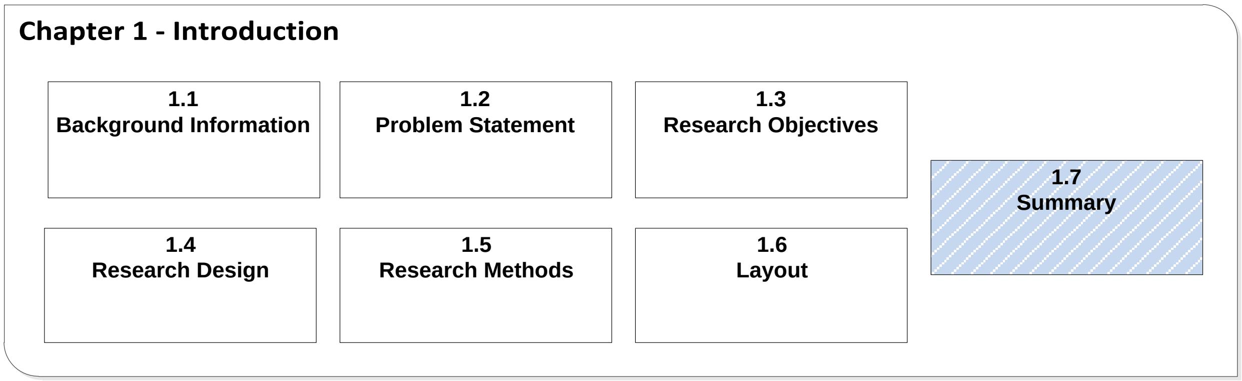

Chapter 1
Introduction
Background, Problem Statement, Research Questions, Research Objectives
Chapter 2
Information Security
Literature Review (Broad Context of Subject Area)
Chapter 3
Information Security Governance
Detailed Review & Content Analysis of Specific Topic Area
Chapter 4
Information Security Governance Components
Detailed Review & Content Analysis of Specific Topic Area
Chapter 5
SMMEs & Related Information Security Management Research
Overview of small, medium and micro sized enterprises and related information security management research conducted within this business type that forms the basis of this work.
(Discussion, critical assessment & evaluation)
Chapter 6
Information Security Governance Framework
Establishes an information security governance framework that caters for the needs of small-to-medium sized enterprises
Chapter 7
Information Security Governance Framework Software Prototype & Evaluation
Demonstrates and evaluates the feasibility of the newly established framework by means of a prototype
(Discussion, screenshots and output generation examples)
Chapter 8
Conclusion
Conclusion, Summary of Contributions, Future Research

Figure 1.2 – Dissertation layout

1.7 Summary

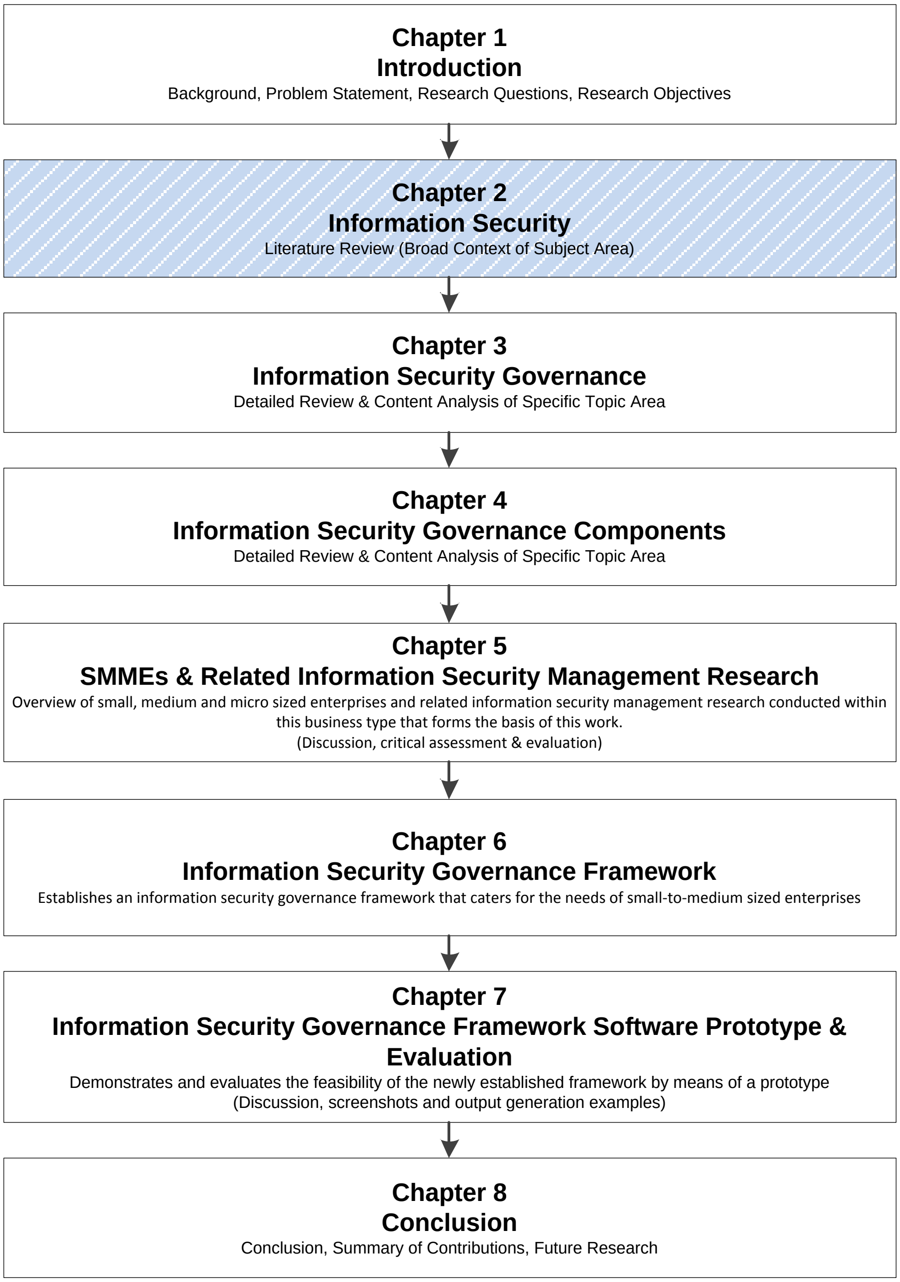


This chapter briefly introduced the concept of information security and its governance in SMMEs, as well as highlighting the various problems that need to be considered in this regard. It should be noted that these enterprises often view information security from a technical point of view, whereas it should rather be addressed as a governance issue. However, research was subsequently presented that indicated that, although some of these enterprises have changed their view, many still experience grave difficulty in adequately addressing and implementing information security owing to the fact that they have limited expertise and resources. These arguments form the basis for conducting this research and support its main objective, which is to develop an information security governance framework supported by a fully functional software prototype, to assist in governing information security with minimal effort and expertise in the SMME sector.

The research design for this dissertation was also discussed, as following the design science guidelines and methodology established by Peffers et al. (2007). This methodology includes the identification and motivation of a business problem; the establishment of the objectives of a solution; the design and development of the solution and, hence, the framework; the demonstration of the solution's feasibility by means of the supportive software prototype; the evaluation of the solution, including the framework and prototype, and the communication of the research findings. Finally, a brief outline of the chapters in this dissertation was given.

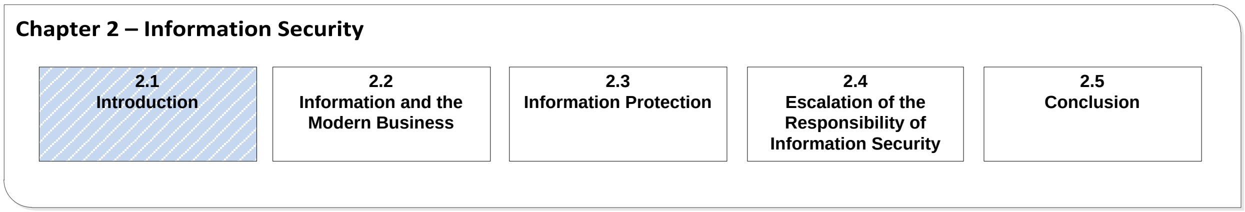
Chapter 2: Information Security

This chapter provides a literature review which examines research on the importance of information in the modern business world, the risks that could manifest in terms of information, as well as the way in which risks to information can be protected against, that is, information security. The fact that the management of information security has been escalated to the top management levels will also be discussed.


Chapter 1
Introduction
Background, Problem Statement, Research Questions, Research Objectives
Chapter 2
Information Security
Literature Review (Broad Context of Subject Area)
Chapter 3
Information Security Governance
Detailed Review & Content Analysis of Specific Topic Area
Chapter 4
Information Security Governance Components
Detailed Review & Content Analysis of Specific Topic Area
Chapter 5
SMMEs & Related Information Security Management Research
Overview of small, medium and micro sized enterprises and related information security management research conducted within this business type that forms the basis of this work.
(Discussion, critical assessment & evaluation)
Chapter 6
Information Security Governance Framework
Establishes an information security governance framework that caters for the needs of small-to-medium sized enterprises
Chapter 7
Information Security Governance Framework Software Prototype & Evaluation
Demonstrates and evaluates the feasibility of the newly established framework by means of a prototype
(Discussion, screenshots and output generation examples)
Chapter 8
Conclusion
Conclusion, Summary of Contributions, Future Research

“Do not figure on opponents not attacking; worry about your own lack of preparation” (Whitman & Mattord, 2012, p. 1).

2.1 Introduction


Chapter 2 – Information Security
2.1 Introduction
2.2 Information and the Modern Business
2.3 Information Protection
2.4 Escalation of the Responsibility of Information Security
2.5 Conclusion

Organisations nowadays are profoundly dependent on information to drive their business processes. In the modern business environment, business processes, supply chains and payment options all require accurate information in order to be ready at short notice. Information is, thus, one of the most critical and valuable resources an organisation can possess (Ernst & Young, 2009). This viewpoint is shared by literature that states that information is the ‘lifeblood’ that keeps modern organisations operational (ISACA, 2012a, p. 13; S. Von Solms & Von Solms, 2008, p. 131). Consequently, if information plays such a crucial role in modern organisations’ operations, then great significance must be placed on the ability to protect it (Whitman & Mattord, 2012, p. 41).

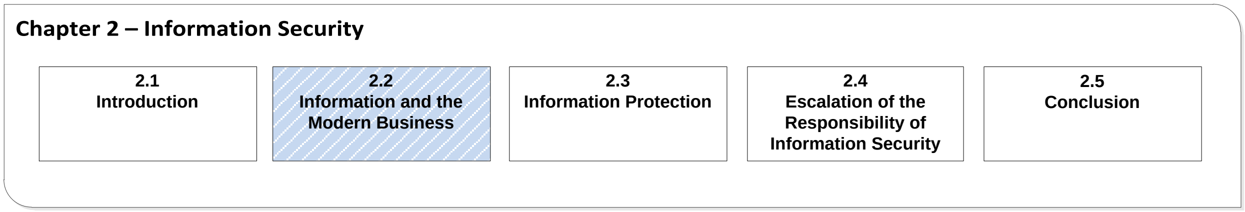
Considering the significance of information in modern businesses, it is impossible for their protection to be ignored (Rees, 2010). Ignorance of the duty to protect information properly could result in calamitous risks, which may include the potential disruption of service, damage to the public image or even the demise of an organisation altogether (S. Von Solms & Von Solms, 2008, p. 1). These calamitous risks form the core focus of information protection, or information security.

Information security consists of the processes and technologies used to offer protection to information. This follows a risk management process by means of which security risks are identified, evaluated and finally mitigated to acceptable levels by means of security controls (Stavroulakis & Stamp, 2010, p. v; S. Von Solms & Von Solms, 2008, pp. 107–124; Whitman & Mattord, 2012, p. 119).

In recent years, as the pervasiveness of information in the modern business has increased, the responsibility for protecting information has received attention from all spheres (Institute of Directors in Southern Africa, 2009a, p. 16). Consequently, an escalation of the responsibility for information security has been witnessed. Where information security was originally viewed as a purely technical measure left to the information technology department, it is nowadays regarded as a management and governance issue that should be addressed by executive management (Gerber & Von Solms, 2005; S. Von Solms, 2006).

These issues will be discussed further in this chapter as follows: Firstly, a discussion on the importance of information, information technology and how it is utilised in modern businesses is provided. Secondly, the discipline involved in protecting information from risks, namely, information security, is introduced and key concepts explained. Finally, a discussion on the escalation of information security responsibility to higher levels of management will follow.

2.2 Information and the Modern Business


Chapter 2 – Information Security
2.1 Introduction
2.2 Information and the Modern Business
2.3 Information Protection
2.4 Escalation of the Responsibility of Information Security
2.5 Conclusion

There are many competing definitions of ‘data’ and ‘information’; and these terms are often mistakenly used interchangeably. A distinction can, however, be made between these two terms: whereas ‘data’ refers to “the computerized representations of models and attributes of real or simulated entities”, ‘information’ may be defined as “data that represents the results of a computational process that has assigned meaning to the data, or a process where human beings has assigned some meaning” (O’Brien & Robertson, 2009). From this definition it is clear that information is data that has been assigned some value.

Information and its use permeate all aspects of modern business. Modern organisations need information to survive and prosper. Therefore, the ability of organisations to endure is directly dependent on their business processes, which have grown to be highly dependent on information (ISACA, 2012a, p. 13). Not only is information entrenched in these processes, but it is also regarded as critical for the supply chains, payments and various other activities that organisations must perform in their regular operations. Although information is essential to the regular operations of a business, its usage can also be seen in the strategic decisions that are made daily by various managers and staff members (O'Brien & Robertson, 2009; R. Von Solms & Von Solms, 2006a). Managers consume information in tremendous volumes from various sources during their daily duties and require it to be accurate, consistent and accessible. If this cannot be assured, the judgements they make may be erroneous and could lead to dire consequences (S. Von Solms & Von Solms, 2008, p. 12).

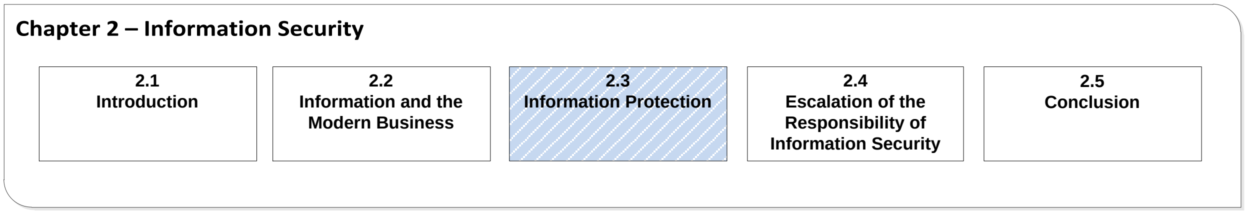
This has consequently led to the realisation that information and its usage have become pervasive in our modern business environments (Institute of Directors in Southern Africa, 2009a, p. 16). This pervasiveness has resulted from the fact that nowadays it is common to find information in many forms in the organisation (S. Von Solms & Von Solms, 2008, p. 12). This realisation has driven, and continues to drive, information as one of the most valuable business assets in modern organisations (S. Von Solms & Von Solms, 2008, p. 7). It should therefore come as no surprise that large investments in terms of time, money and energy are made to capture, generate and distribute information.

The computer systems that drive information, known as information systems, make up a large portion of the investments made by organisations (Ernst & Young, 2009). An information system (IS) is an organised combination of people, hardware, software, communication networks, processes and data resources that collects, transforms and disseminates valuable information in an organisation (Whitman & Mattord, 2012, p. 16). These ISs and the architecture on which they operate are commonly referred to as the information technology (IT) of an organisation. The advent of IT has had a profound impact on modern business, as almost all information in modern businesses is today created, stored, transmitted and maintained digitally. Accordingly, IT affects all aspects of modern business from executive management down to the operational levels. From the time that information is created to the moment that it is destroyed, IT plays a significant role. Consequently, without the driving force of IT in an organisation, information might not be accessible or might become impossible to obtain. It is therefore believed that IT is a major contributor to the competitiveness of modern business (ISACA, 2012a, p. 57).

It can therefore be stated that information, and the technology that drives it, is essential for obtaining and maintaining the competitive advantage and wellbeing of an organisation. This is supported by Brotby (2009, p. xiii), who states that "in many organisations, information is the business". Thus, the dependence on information and IT for the wellbeing of modern organisations should be recognised and at best protected as far as possible. Accordingly, if for any reason an organisation's information is disclosed, inaccurate or unavailable its reputation could tarnish rapidly (Whitman & Mattord, 2012, p. 11).

The importance and protection of information cannot therefore be understated and organisations should be mindful of their duties and obligations in this regard.

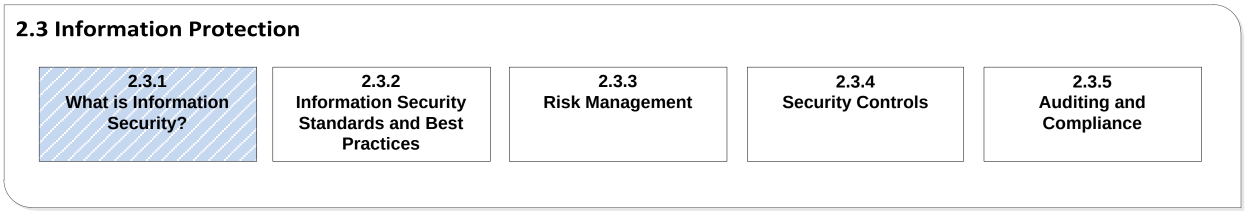
2.3 Information Protection


Chapter 2 – Information Security
2.1 Introduction
2.2 Information and the Modern Business
2.3 Information Protection
2.4 Escalation of the Responsibility of Information Security
2.5 Conclusion

Security breaches during the use and distribution of information have drastically increased since the turn of the century, as many organisations have become dependent on information and the IT architecture (Smedinghoff, 2008). These breaches have an extraordinary propensity to impact negatively on the organisation's reputation, profitability, customer confidence and overall economic growth (ISO/IEC 27002, 2005, p. viii; Richardson, 2008).

It is therefore fundamental for organisations to realise that their ability to attain and sustain a competitive advantage in highly volatile, demanding and uncertain markets is directly dependant on their ability to protect their information and IT (Dlamini, Eloff, & Eloff, 2009; ISACA, 2012a, p. 13). As Dlamini et al. (2009, p. 2) state “it is not by mistake that information protection has become a common topic not only to the world of computing, but also to various other industries”. The technologies and processes used to provide such protection for information are collectively known as *information security*.

2.3.1 What is Information Security?


2.3 Information Protection
2.3.1 What is Information Security?
2.3.2 Information Security Standards and Best Practices
2.3.3 Risk Management
2.3.4 Security Controls
2.3.5 Auditing and Compliance

The protection of information was viewed as essential even prior to the invention of the computer; from the time that information began to be transmitted, stored and processed, it required protection. This protection moved from protecting the secrecy of handwritten messages, to protecting the contents of telephone conversations and later to protecting data in the world of computing. The main concern of information security has, however, always been the same: protecting the integrity and confidentiality of information. In order to fully grasp the term ‘information security’, one first needs to understand what security is.

Generally, the term ‘security’ may be defined as “the quality or state of being secure – to be free from danger” (Whitman & Mattord, 2012, p. 8). This definition thus implies that protection must be provided by applying security in order to ensure that intentional or accidental danger is mitigated. In order to provide this protection, multiple dimensions of security may need to be realised. These include security governance, best practices, standards, auditing, compliance, policies and many more (S. Von Solms, 2001).

The terms ‘information assurance’, ‘computer security’ and ‘information security’, to mention but a few, are often used to refer to the same concept(s). Although some might believe that these terms are similar, there are underlying differences between them. Information assurance can be explained as the “management of all risks concerning information”, which involves taking protective measures to address the confidentiality, integrity and availability of information (Clinch, 2009, p. 12). In contrast, computer security is “the management of the security of the computers and networks that hold and convey information” (Clinch, 2009, p. 12). Finally, ‘information security’ can be clearly distinguished as “the active protection of information, however stored or conveyed, to ensure it is available only to authorized users at the time they required it, with appropriate levels of integrity” (Clinch, 2009, p. 12). Thus, these concepts, although closely related, do indeed vary in meaning. Consequently, the remainder of this work will follow the definition of information security closely so as to avoid confusion.

Many supporting definitions for information security can also be found in the literature. ISO/IEC 27002 (2005, p. viii) defines information security as “the protection of information from a wide range of threats in order to ensure business continuity, minimize risk, maximize return on investment and business opportunities”. The definition continues by indicating that information security is realised through the implementation of suitable controls, including policies, procedures and various other components. Andress (2011, p. 2) supports this notion of protecting against threats and risks by stating that information security is “the protection of information against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional”. Whitman and Mattord (2012, p. 164) highlight the fact that information security affords assurances by stating that information security is a “well-informed sense of assurance that the information risks and controls are in balance”.

It can therefore be concluded from these definitions that information security is a process that affords the assurance that the key characteristics of information will be actively protected against risks by means of security controls. Although information security is often viewed as single concept, in reality it consists of many subcomponents, as outlined by Figure 2.1 below. These subcomponents include, among others, management aspects, computer and data security, policies establishing vision and guidelines and, finally, network security. These all work together to ensure the adequate protection of information (Whitman & Mattord, 2012, p. 9).

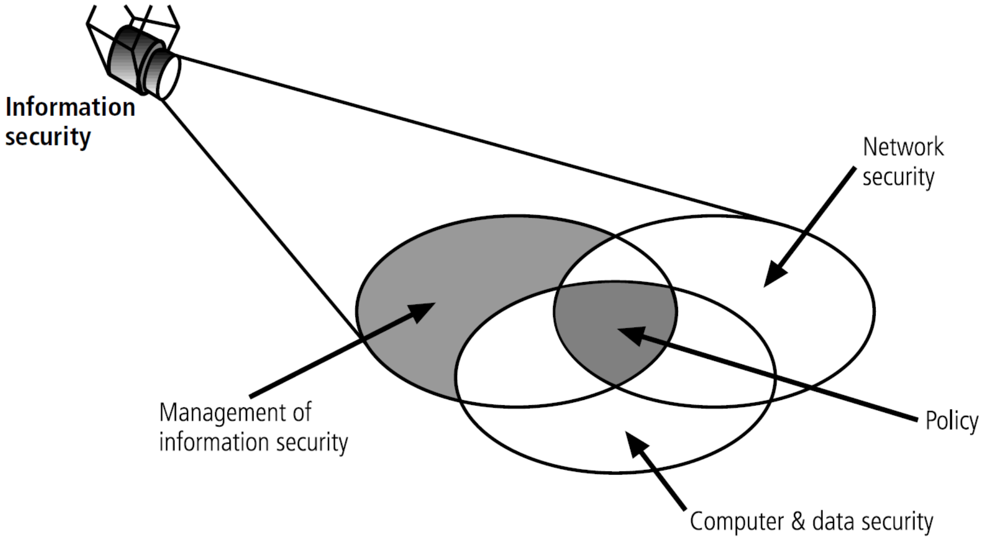
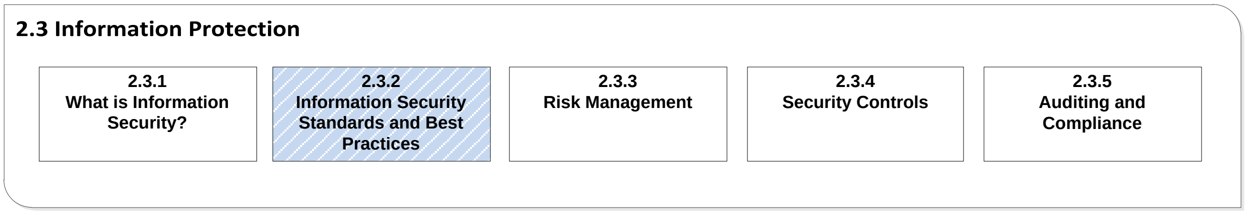


Figure 2.1 – Components of information security (Whitman & Mattord, 2012, p. 9)

The protection of information against risks plays a pivotal role in ensuring that benefits such as competitive advantages, increased cash flow and legal compliance are attained (ISO/IEC 27002, 2005, p. viii). In the past, where information was perhaps not as pervasive, information security was often seen as a by-product. This led organisations to leave information security to be addressed by the IT department. Today, however, this viewpoint has changed and, consequently, information security has become an integral part of business operations (Dlamini et al., 2009). It has therefore been realised that information security is not an IT problem, but rather a business and management problem that all businesses, irrespective of size, have a responsibility to address (ISO/IEC 27002, 2005, p. viii; Vacca, 2009, p. 225).

Many people, managers included, believe that merely protecting information by implementing information security is sufficient; however, if the protection of information is not managed properly it could fail altogether or lead to unwelcome consequences (S. Von Solms & Von Solms, 2008, p. 14). Organisations that do not realise this continue to experience damaging security failures and losses owing to the risks that information faces (Brotby, 2009, p. xiii). Consequently, many standards and best practices for information security management have been established which may provide guidance for organisations in this regard.

2.3.2 Information Security Standards and Best Practices


2.3 Information Protection
2.3.1 What is Information Security?
2.3.2 Information Security Standards and Best Practices
2.3.3 Risk Management
2.3.4 Security Controls
2.3.5 Auditing and Compliance

Many standards and best practices exist to aid information security management in organisations. These standards and best practices are provided by reputable institutions such as the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), the National Institute of Standards and Technology (NIST) and the Information Security Forum (ISF). Other institutions include the British Standards Institute (BSI) and the South African National Standards Institute (SANS).

The ISO, together with the IEC, aims to promote worldwide standards and practices for industry and commerce. In order to address the rapid growth of the internet and the dependence of modern business on information, these institutions have introduced the ISO/IEC 27000 series (see Table 2.1 below) to provide a methodical and effective approach to information security management. Of specific interest to this work are the ISO/IEC 27001 (2005) and 27002 (2005) standards, and these will be discussed below.

Table 2.1 – ISO/IEC 27000 series of information security standards

Published Standards	Year Published	Title of Standard
ISO/IEC 27000	2009	Information technology – Security techniques – Information security management systems – Fundamentals and vocabulary
ISO/IEC 27001	2005	Information technology – Security techniques – Information security management systems – Requirements
ISO/IEC 27002	2005	Information technology – Security techniques – Code of practice for information security management
ISO/IEC 27003	2010	Information technology – Security techniques – Information security

		management system implementation guidance
ISO/IEC 27004	2009	Information technology – Security techniques – Information security management – Measurement
ISO/IEC 27005	2008	Information technology – Security techniques – Information security risk management
ISO/IEC 27006	2007	Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems.

ISO/IEC 27001 (2005) is entitled ‘Information technology – Security techniques – Information security management systems – Requirements’. This standard was originally published as BS7799 Part 2 by BSI, but was revised and accepted as an international standard in October 2005. The objective of this standard is “to provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an Information Security Management System” (ISO/IEC 27001, 2005, p. v).

The standard employs the well-known plan–do–check–act (PDCA) model to structure the processes involved with the implementation of an information security management system. The standard also reveals the principles of the Organisation for Economic Co-operation and Development (2004) guidelines, which include awareness, responsibility, response, risk assessment, security design and implementation and security management.

Furthermore, this standard recommends the use of ISO/IEC 27002 (2005) as a guide for controls, control selection and control implementation. Therefore, an organisation wanting to comply with ISO/IEC 27001 (2005) would need to refer to both standards. It should be noted, however, that ISO/IEC 27002 (2005) is a code of practice and therefore an organisation cannot comply with it.

ISO/IEC 27001 (2005) also requires organisations to perform risk management which entails the selection and operation of information security controls. Although this standard specifies the steps to be followed when carrying out risk management, it does not provide detailed guidance in this regard.

ISO/IEC 27002 (2005) is entitled ‘Information technology – Security techniques – Code of practice for information security management’. This standard was published in 2005 and replaced the ISO/IEC 17799 standard which was originally published as BS7799 Part 1 by BSI. This standard provides fundamental control mechanisms that may be implemented in accordance to ISO/IEC 27001 (2005). The implementation of ISO/IEC 27002 (2005) therefore entails the identification of applicable controls from those provided and, subsequently, executing them in order to mitigate identified risks, thereby protecting the confidentiality, integrity and availability of information. This process is generally referred to as risk management and forms a core component of any information security management implementation or system.

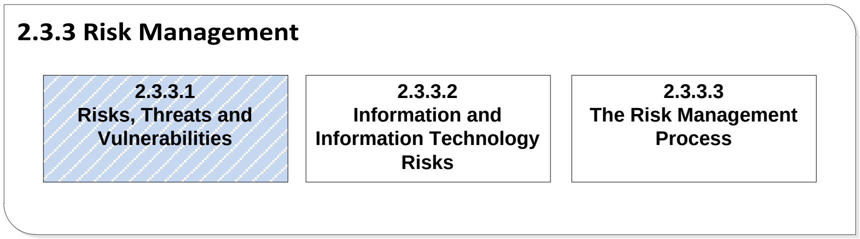
It can, therefore, be concluded that the management of information security is essential in ensuring adequate protection for information. Many standard and best practices exist to aid organisations in this regard. Two standards that will play a prominent role in this work are ISO/IEC 27001 (2005) and ISO/IEC 27002 (2005), as both provide detail on the management of information security. Both of these standards also emphasise that in order for information security management to be successful, risk management is vital and must be addressed.

2.3.3 Risk Management

2.3 Information Protection
2.3.1 What is Information Security?
2.3.2 Information Security Standards and Best Practices
2.3.3 Risk Management
2.3.4 Security Controls
2.3.5 Auditing and Compliance

According to ISO/IEC 27002 (2005, p. 2), risk management refers to “the coordinated activities to direct and control an organisation with regard to risk”. The aim of these coordinated activities is to identify, control and minimise the impact of threats (Rainer & Cegielski, 2010, p. 99) by seeking suitable controls which can mitigate risks to an acceptable level (Rainer & Cegielski, 2010, p. 101; S. Von Solms & Von Solms, 2008, p. 107).

2.3.3.1 Risks, Threats and Vulnerabilities


2.3.3 Risk Management
2.3.3.1 Risks, Threats and Vulnerabilities
2.3.3.2 Information and Information Technology Risks
2.3.3.3 The Risk Management Process

“The term risk dates back to the seventeenth century when mathematicians calculated the risk of winning or losing when gambling” (S. Von Solms & Von Solms, 2008, p. 107). A risk can be described as “a combination of the probability of an event and its subsequent impact” (ISO/IEC 27002, 2005, p. 2). Today, the term ‘risk’, although still the same in definition, has acquired a totally negative connotation when referring to outcomes of risk in engineering and science, with particular reference to the hazards posed by modern technological developments.

For a risk to exist, both vulnerability and a threat must be present (Andress, 2011, p. 10). A threat is anything that has the potential to cause harm; while a vulnerability refers to weaknesses that can be exploited to generate the harm (Vacca, 2009, p. 383). It can therefore be stated that threats and vulnerabilities are two sides of the same coin: threats are the potential actions that will follow the path of least resistance to the greatest vulnerabilities (Gregory, 2003, p. 11), as shown in Figure 2.2 below.

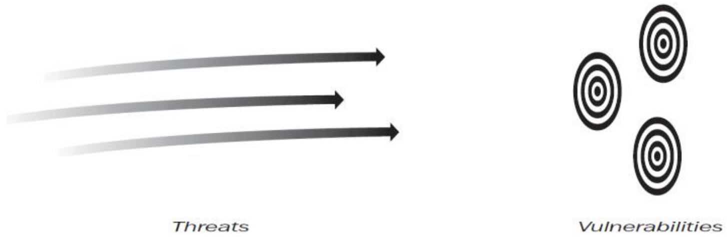


Figure 2.2 – Threats and vulnerabilities (Gregory, 2003, p. 11)

The threat process depicted in Figure 2.3 recognises the relationship that exists between a threat, vulnerability and the resultant risk. As shown, a threat agent (the aspect wanting to cause harm) gives rise to a threat that exploits vulnerability in an asset. This then leads to a risk for which protection, in the form of security controls, must be ensured. The risk may result in an impact on an asset, in this case related to information, and results in the exposure of the asset to the threat.

In controlling or mitigating a risk, one usually attempts to attain one of three general outcomes (S. Von Solms & Von Solms, 2008, p. 108):

- reduce the potential impact
- reduce the probability of the threat being realised
- a combination of both of the above.

Figure 2.3 below highlights the fact that risks are usually controlled or mitigated by selecting, implementing and maintaining suitable security controls. Note that the terms 'safeguard', 'counter-measure' and 'security control' are often used interchangeably to refer to the same concept. In this work the term 'security control' will be used to ensure consistency and avoid confusion.

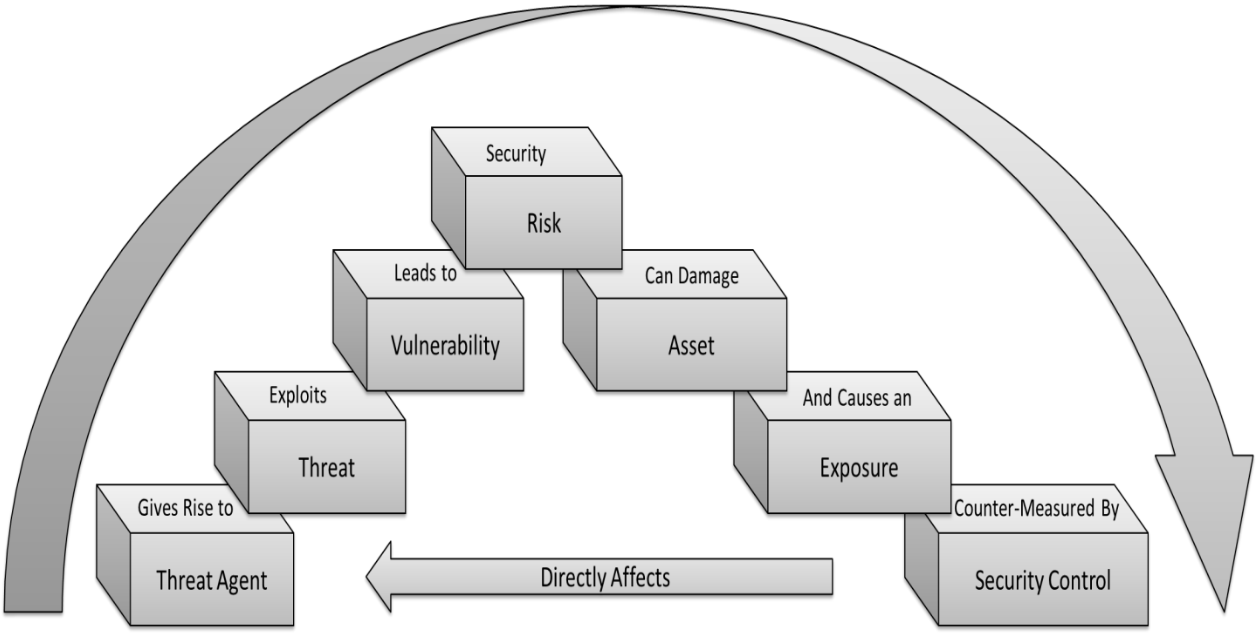
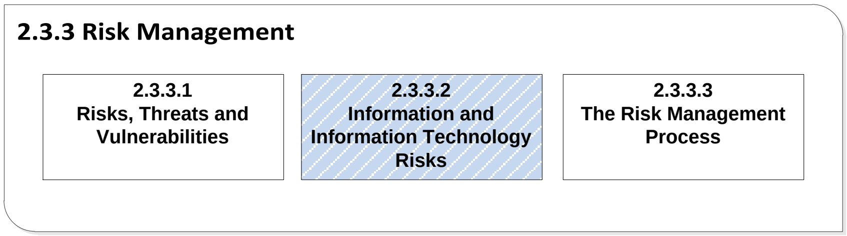


Figure 2.3 – The threat process (adapted from Vacca, 2009, p. 229)

Risks are present in all activities carried out in life, and may originate from business, finance, the environment and even legal obligations. Accordingly, these need to be identified and duly managed, specifically those related to information and IT.

2.3.3.2 Information and Information Technology Risk


2.3.3 Risk Management
2.3.3.1 Risks, Threats and Vulnerabilities
2.3.3.2 Information and Information Technology Risks
2.3.3.3 The Risk Management Process

In an organisation there are many types of risk that must be managed (S. Von Solms & Von Solms, 2008, p. 7). Among these, information and IT-related risks are most important; if such risks are realised it could result in the organisation coming to a standstill (ISO/IEC 27002, 2005, p. viii; S. Von Solms & Von Solms, 2008, p. 7).

Information is indispensable to businesses in our modern society and therefore a key asset of any organisation (S. Von Solms & Von Solms, 2008, p. 139). Therefore, as has already been discussed, its protection should be seen as a critical requirement of modern business, in particular in view of the interconnected nature of business today. Although this interconnectedness continues to provide many advantages, it does, however, also pose risks (Vacca, 2009, p. 229), as information is exposed to many risks when processed, stored and transferred using IT (Vacca, 2009, p. 228; Whitman & Mattord, 2012, pp. 42–43).

Generally, information and IT risks may be categorised into a number of broad categories, including the following (National Archives (Great Britain), 2008):

- Governance and culture
  - lack of comprehensive review and control
  - third parties not performing their duties
  - new business processes not taking information risk into account

- Information management and information integrity
    - critical information being wrongly destroyed
    - inaccurate information
- The human dimension
    - external parties obtaining information illegally
    - insiders performing deliberate acts
    - insiders acting in error
- Information availability and use
    - inappropriate disclosure of sensitive personal information
    - failure to realise the value of information assets
    - failure to allow information to be obtained by the rightful person only.

Unmitigated or uncontrolled risks may result in information and IT security breaches not only having a serious financial impact on an organisation, but they can also lead to litigation and other grave consequences (Vacca, 2009, p. 231). Such consequences have been shown to result in a tarnishing of corporate reputation, as well as loss of business and payment of legal fees (Dlamini et al., 2009; Vacca, 2009, p. 231). The CSI/FBI Security Report (Richardson, 2008)[1] highlights some key findings on IT security breaches:

- Financial fraud is costing organisations dearly, with an average reported loss of close to US$500 000 in the United States of America for 2007.
- Bots within networks were reported to cost organisations an average of nearly US$350 000 in the United States of America for 2007.

These findings are further supported by Figure 2.4, which shows the average losses, in thousands of dollars, experienced for information and IT security breaches each year during the period 1999 to 2008 in the United States of America. The figure indicates that an average loss of US$927 500 was experienced per year during this period.

[1] Note that the 2010/11 Report did not provide monetary values for security breaches; therefore the 2008 report was used.

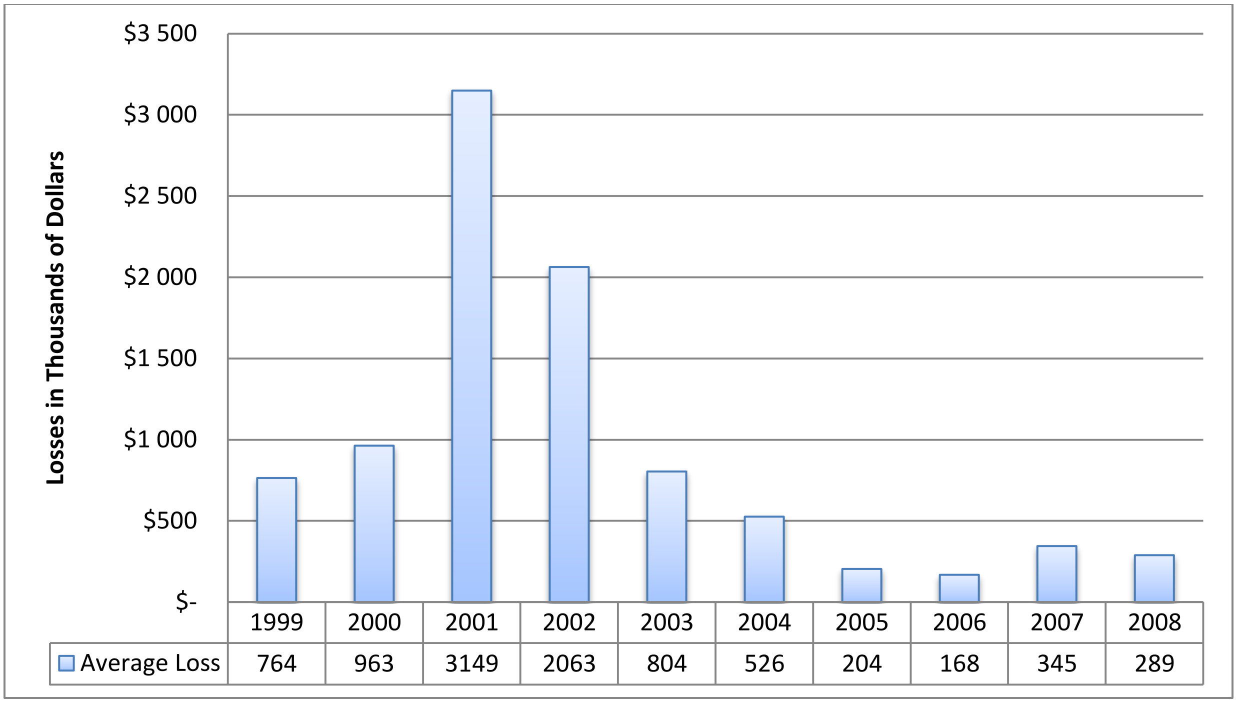


Figure 2.4 – Average losses per year (Richardson, 2008)

A number of case studies also indicate the effects of information risk (National Archives (Great Britain), 2008):

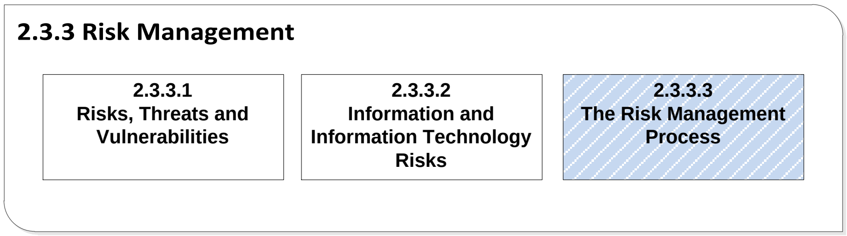
- In December 2007, Norwich Union Life was fined £1,26 million for failing to properly assess the risks posed by its IT systems and controls, which resulted in financial crime.
- In 2004, Banc of America Securities LLC (BAS) paid US$10 million to settle charges that it failed to preserve or produce emails and other documents during an investigation by the US Securities and Exchange Commission (SEC).
- In 2002, SEC, the New York Stock Exchange and NASD took joint action against five broker-dealers for violating record-keeping requirements. Deutsche Bank Securities Inc., Goldman, Sachs & Co., Morgan Stanley & Co. Inc., Salomon Smith Barney Inc. and US Bancorp Piper Jaffray Inc. were fined US$8,25 million – US$1,65 million each – for failing to preserve emails.
- In 2006, Morgan Stanley & Co. Inc. paid US$15 million to settle charges of repeatedly failing to produce emails and over-writing back-up tapes requested in analyst investigations by SEC between 2000 and 2005.

To conclude, in underlining the dangers of security breaches, Vacca (2009, p. 231) states:

- “How much would it cost your organisation if your e-commerce website went down for 12 hours?
- What if your mainframe database was not accessible for an entire afternoon?
- What if your website was defaced and rerouted all your customers to a site infected with malicious code?
- Would any of these scenarios significantly impact your organisation?”

These questions attempt to illustrate the severe risks that are faced by an organisation if not controlled or mitigated. Consequently, organisations should ensure that a structured process, known as risk management, is put in place in order to allow such risks to be identified, evaluated and, finally, mitigated to alleviate the effects that have been outlined.

2.3.3.3 The Risk Management Process


2.3.3 Risk Management
2.3.3.1 Risks, Threats and Vulnerabilities
2.3.3.2 Information and Information Technology Risks
2.3.3.3 The Risk Management Process

Risk management can be viewed as a comprehensive process which, typically, includes risk assessment, consisting of risk analysis and evaluation, and risk treatment (S. Von Solms & Von Solms, 2008, p. 120). As shown in Figure 2.5, after suitable controls have been implemented there may still be residual risk.

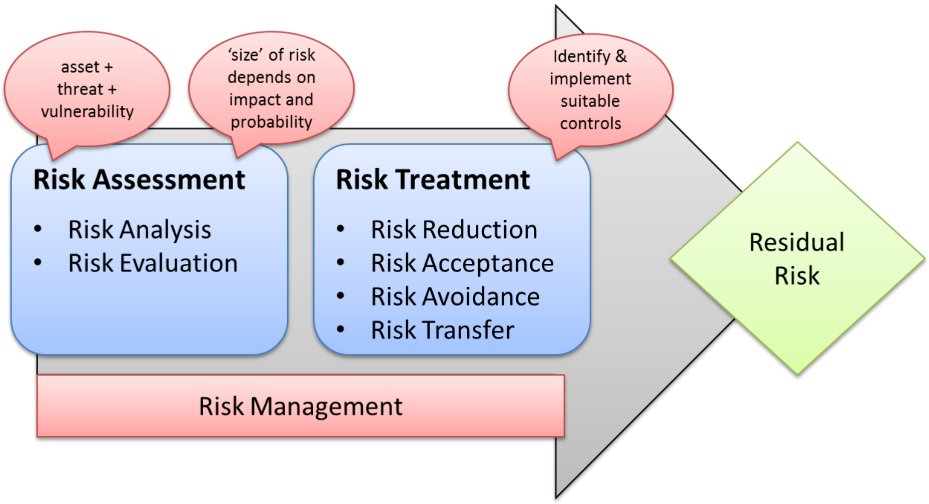


Figure 2.5 – Risk management process (Futcher, 2011, p. 90)

Consequently, risk management, as stated, comprises two processes, namely, risk assessment and risk treatment. Risk assessment refers to the overall process comprising risk analysis and risk evaluation (S. Von Solms & Von Solms, 2008, p. 111), which allows for threats and vulnerabilities to be identified, existing security controls and their effect on risks to be known, the potential impact on information assets to be estimated and derived risks to be prioritised and addressed (ISO/IEC 27005, 2008, p. 10). Whereas risk analysis is concerned with the identification of risks and its sources, risk evaluation aims to assign a value to a risk. This value of a risk is often referred to in terms of its size.

Once the activities of risk assessment have been carried out, risk treatment should happen as shown in Figure 2.6 below. Risk treatment, also referred to as risk mitigation, can be viewed as "the process of selecting and implementing measures to modify risk" (ISO/IEC 27002, 2005, p. 2). From this definition it can be inferred that risk treatment has two main functions: firstly, identifying and selecting controls to prevent identified threats from occurring; and secondly, implementing controls as a means of protection should these threats become a reality (Rainer & Cegielski, 2010, p. 101). There are several risk treatment strategies that an organisation may adopt. These include the following (ISO/IEC 27002, 2005, p. 5):

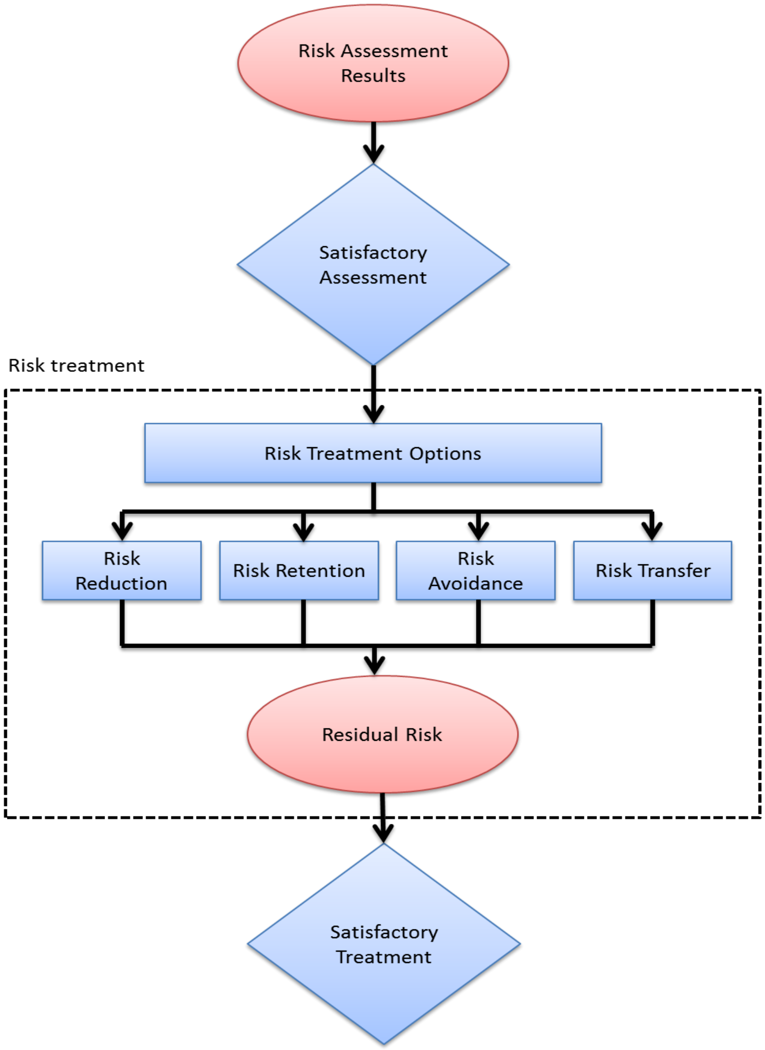


Figure 2.6 – Risk treatment process (adapted from ISO/IEC 27005, 2008, p. 18)

- Risk reduction
  - applying appropriate controls to reduce the risks
- Risk retention
  - knowingly and objectively accepting risks, providing they clearly satisfy the organisation’s policy and criteria for risk acceptance
- Risk avoidance
  - avoiding the risks by not allowing actions that would cause the risks to occur
- Risk transfer
  - transferring the associated risks to other parties

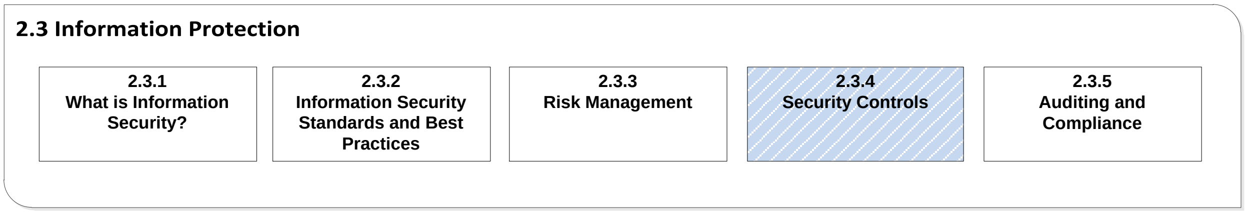
It should be noted that even with the introduction of security controls during the risk treatment process, not all risks can be fully controlled or mitigated and, consequently, residual risk is generally present (Whitman & Mattord, 2012, p. 144). Residual risk can therefore be defined as the "remaining risk after controls have been implemented" (S. Von Solms & Von Solms, 2008, p. 111). Such a residual risk, if shown to be small enough, would normally be acceptable to the organisation.

The process of risk management can therefore be concluded as contributing to the following aspects (ISO/IEC 27005, 2008, p. 4):

- "Risks being identified;
- Risks being assessed in terms of their impact to the business and the likelihood of their occurrence;
- The likelihood and impact of these risks being communicated and understood;
- Priority order for risk treatment being established;
- Priority for actions to reduce risks occurring;
- Stakeholders being involved when risk management decisions are made and kept informed of the risk management status;
- Effectiveness of risk treatment monitoring;
- Risks and the risk management process being monitored and reviewed regularly
- Information being captured to improve the risk management approach; and
- Managers and staff being educated about the risks and the actions taken to mitigate them."

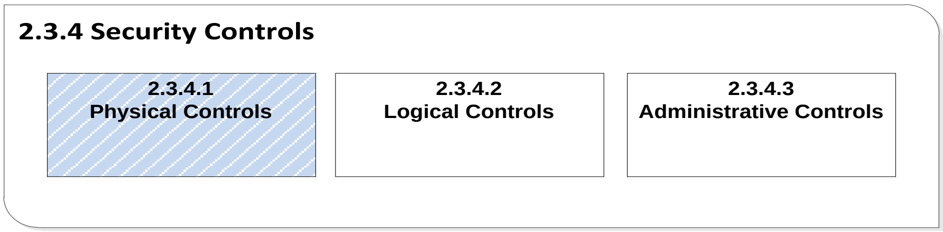
The Queensland Government states that "information security risk management adapts this generic process of risk management, and applies it directly to information assets and the information infrastructure of the organisation" (Queensland Government, 2001, p. 5). This literature source continues by indicating that, if information security risk management is effectively introduced and used, then it provides a tool in an organisation's arsenal for proactively managing and protecting its information (Queensland Government, 2001). However, central to this management and protection of information, is the notion that risk treatment by means of security controls should be introduced. Hence, the concept of security controls is introduced in the following subsection.

2.3.4 Security Controls


2.3 Information Protection
2.3.1 What is Information Security?
2.3.2 Information Security Standards and Best Practices
2.3.3 Risk Management
2.3.4 Security Controls
2.3.5 Auditing and Compliance

In order for risks to be mitigated or controlled, certain measures must be put in place (S. Von Solms & Von Solms, 2008, p. 108). These measures are commonly referred to as 'security controls' and may be of a physical, technical or administrative nature (Andress, 2011, p. 11). Such controls allow for accidental hazards to be prevented, intentional acts to be deterred, problems to be detected as early as possible, damage recovery to be implemented and problems to be corrected (Rainer & Cegielski, 2010, p. 101).

2.3.4.1 Physical Controls

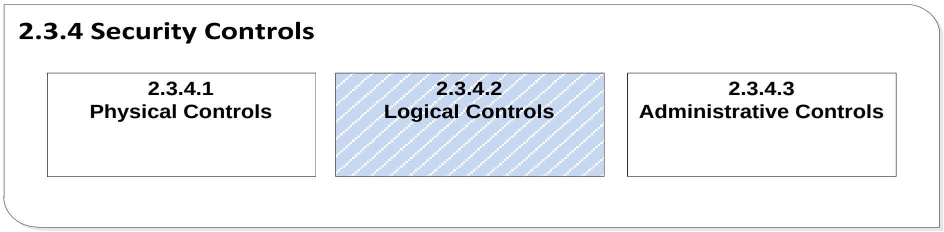


Physical controls form the first level of defence for an organisation. Such controls prevent access to facilities by unauthorised individuals (Rainer & Cegielski, 2010, p. 101). Accordingly, these controls regulate access in and out of organisational environments (Vacca, 2009, p. 232). Such controls are the easiest and least expensive to implement, but are often also the most effective (Pfleeger & Pfleeger, 2006, p. 27). Common physical controls include items such as walls, doors, fencing, gates, locks, badges, guards, bollards, cameras and alarm systems (Andress, 2011, p. 11; Rainer &

Cegielski, 2010, p. 101). Andress (2011, p. 11), however, also mentions that physical controls include the measures required to maintain the physical environment in organisations, including heating, air-conditioning systems, fire-suppression systems and backup power generators.

Many believe that physical controls do not play a vital role in an organisation's security, but they are actually the most critical components (Andress, 2011, p. 11). They can be considered critical owing to the fact that if one cannot guarantee or protect the physical environment in an organisation, then any other controls that are added would be immaterial (Andress, 2011, p. 11).

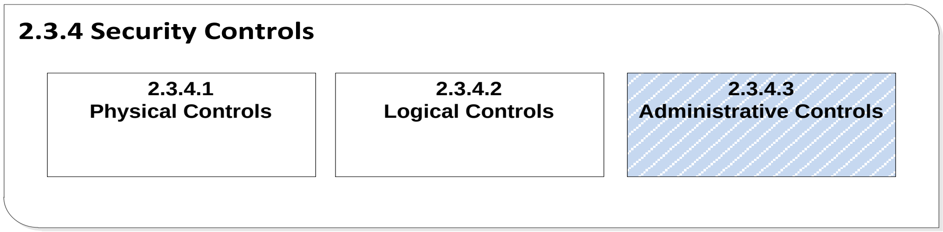
2.3.4.2 Logical Controls



Logical controls, often referred to as technical controls, are those controls that ensure that the systems, networks and environments in an organisation that process, transmit and store information are protected against both unintentional and deliberate potential security violations (Andress, 2011, p. 11; Vacca, 2009, p. 232). These controls typically include passwords, encryption, logical access control, firewalls and network intrusion detection systems.

Andress (2011) states that "if logical controls are implemented properly and are successful, an attacker or unauthorized user cannot access [an organisation's] applications and data without subverting the controls that we have in place" (Andress, 2011, p. 11). Therefore, these controls allow for logical separation, also referred to as the principle of least privilege, which aims to prevent unauthorised activities from taking place by limiting the privileges of individuals, programs and systems (Andress, 2011, p. 11; Vacca, 2009, p. 232).

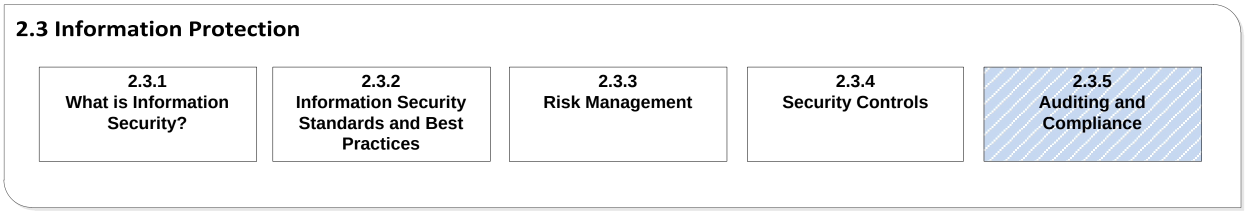
2.3.4.3 Administrative Controls



It should be noted that protection cannot be assured by physical and logical controls only; therefore administrative controls must also be present in an organisation (Jansson, 2011, p. 22). Administrative controls, also referred to as management controls, provide an organisation with a framework according to which it can manage the conduct of its employees (Vacca, 2009, p. 232). Typical controls would include items of a paper nature, such as rules, laws, policies, procedures and guidelines (Andress, 2011, p. 11). These items are crucial as they set the vision for implementing physical and technical controls (Vacca, 2009, p. 232).

Note that administrative controls offer clear guidance to employees on how they should act when confronted with a potential security breach (Vacca, 2009, p. 232). Unfortunately, organisations have found that if they cannot enforce compliance with these controls, then their value is drastically diminished (Andress, 2011, p. 12). This often leads to a false sense of security (Andress, 2011, p. 12), where management of an organisation trusts that its employees are operating in a safe and secure manner, but in actual fact they might not. This lack of compliance often results in serious consequences for organisations (Andress, 2011, p. 12). It can therefore be stated that “having controls that are not monitored or enforced is tantamount to having laws but no police” (West, 2008, p. 40).

2.3.5 Auditing and Compliance

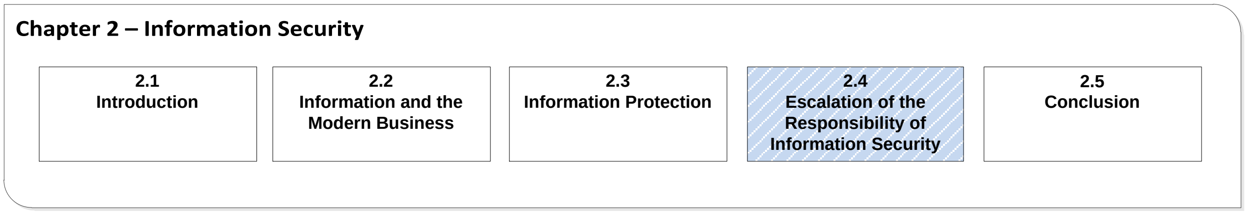

2.3 Information Protection
2.3.1 What is Information Security?
2.3.2 Information Security Standards and Best Practices
2.3.3 Risk Management
2.3.4 Security Controls
2.3.5 Auditing and Compliance

Information security practices suggest that any security controls implemented should be audited regularly to ensure that they are effective and operating efficiently (S. Von Solms & Von Solms, 2008, p. 127). R. Von Solms and Von Solms (2006a, p. 411) state that “you can only manage what you can measure”. In addition, threat agents are constantly finding more sophisticated means of using threats to exploit vulnerabilities (Richardson, 2008). Therefore, it is imperative that the physical, logical and administrative controls that are implemented and enforced be complied with and updated regularly to ensure adequate protection (S. Von Solms & Von Solms, 2008, p. 127). It is crucial that organisations realise the importance of this, as one cannot defend against risks that are unfamiliar or not known. For example, if a person’s logon and access rights are still active six months after they have left the organisation, this poses an unacceptable risk for the organisation. It is for this reason that S. Von Solms and Von Solms (2008, p. 93) state that auditing and compliance checking must be performed on a regular, if not a real-time, basis.

In the event that the organisation follows the guidelines provided by a standard, such as ISO/IEC 27002 (2005), then a supportive certification standard (in this case ISO/IEC 27001 (2005)) may be used to check for compliance and to perform a security audit. Such a security audit will generally expose the flaws and areas that are lacking in the organisation’s security processes. Whitman and Mattord (2012, p. 545), however, state that organisations must remain vigilant in updating their information security programmes so as to embrace the latest standards, best practices and technical products, as new risks and improved protection techniques are born every day.

Although auditing and compliance are vital in ensuring adequate protection for information, it must be realised that management needs assurance that its information will be available, correct and confidential at all times. It is, thus, essential that the results of audits are reported to management and that the overall security decisions be contingent on their insight.

2.4 Escalation of the Responsibility of Information Security


Chapter 2 – Information Security
2.1 Introduction
2.2 Information and the Modern Business
2.3 Information Protection
2.4 Escalation of the Responsibility of Information Security
2.5 Conclusion

Information security has seen tremendous advances and changes over the past few years (Gerber & Von Solms, 2001; S. Von Solms, 2006). In the computer-centric era, up to the early eighties, information security was mainly characterised by a very physical approach with physical controls taking the primary focus. It was believed that if computer centres and equipment were physically secured they were, in fact, safe. This resulted in information security being applied mainly with the aid of physical controls such as surveillance and access control (Gerber & Von Solms, 2001). This approach resulted in the responsibility for information security being placed on the staff members who were directly involved with the few computer systems that organisations controlled.

This viewpoint, however, changed with the introduction of multiprocessing and distributed computing systems during the IT-centric era witnessed during the middle nineties (Gerber & Von Solms, 2001). Suddenly protection of information could not be provided by physical measures alone, as interconnectivity started to increase. Consequently, a more technical approach to information security was taken with the advent of increasingly technical measures being applied, including user identification and authentication, access controls, encryption of communication lines, among others, as information resources faced risks from both internal and external locations (S. Von Solms & Von Solms, 2008, p. 21; S. Von Solms, 2006). Furthermore, the responsibility for information security shifted; where information security had been originally primarily computer operator based, the ownership of information and protection of information now became the responsibility of IT managers.

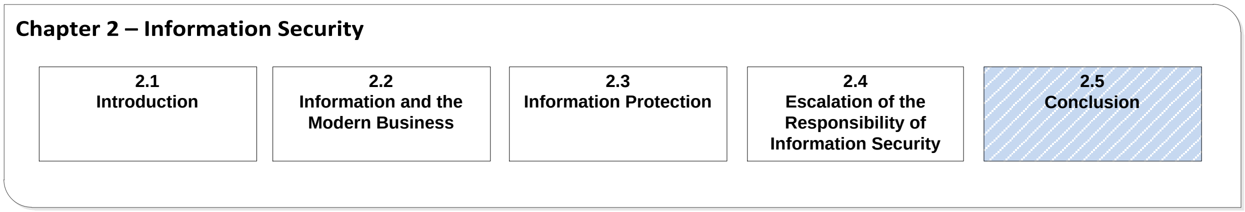
This approach has changed further with the advent of the information-centric era, which occurred after the turn of the century when many organisations became dependent on information that was being used throughout the business processes (Gerber & Von Solms, 2005). Not to mention the increased usage of cloud computing, having seen tremendous growth over the past few years, in addition to the notion of ‘bring your own device’ (BYOD) which is allowing staff to add their own personal devices to the corporate network infrastructure. This dominance of information in the modern organisation has led to the realisation that not only is information protection paramount, but also that management is crucial in this regard (Von Solms, 2006). This understanding has resulted in the introduction of many administrative controls that can be used to manage information security, including policies, procedures, best practices and standards. Consequently, the responsibility for information security has transitioned from IT managers to executive management.

Although information security has remained an operational and management issue, the continued necessity for information has led, in recent years, to the recognition that information security should also be addressed as a governance matter (Brotby, 2009, p. 9; S. Von Solms & Von Solms, 2008, p. iv). Brotby (2009, p. xiv) observes that if governance of information security cannot be ensured, continued chaotic, increasingly expensive and marginally effective fire-fighting with regard to information risks may result. Furthermore, the allocation of security resources may remain haphazard and unrelated to the risks and consequences experienced (Brotby, 2009, p. xv). Accordingly, breaches and losses may continue to grow and regulatory compliance may be costly to address (Brotby, 2009, p. xv). Finally, it has been found that if information security is proven to be ineffective as a result of negligence, and due care is not being taken by means of governance, then corporate reputation may suffer, not to mention the fact that the executive management could be held legally liable (R. Von Solms & Von Solms, 2006b).

In contrast, researchers have found that if information security governance has been applied and is complete, many benefits may be gained and many of the above-mentioned problems alleviated (S. Von Solms & Von Solms, 2008). These benefits may include an organisation being perceived as more trustworthy by its customers and stakeholders, a reduction in the uncertainty of business operations, an increase in organisational worth and, most importantly, the alignment of security with business objectives (Brotby, 2009, pp. 11–15).

It can thus be concluded that the nature of information security, as well as the responsibility therefore, has indeed escalated over time and that it has come to reside squarely on the shoulders of executive management. Executive management should therefore realise that it plays a critical role in information security and, subsequently, in the wellbeing of the organisation.

2.5 Conclusion


Chapter 2 – Information Security
2.1 Introduction
2.2 Information and the Modern Business
2.3 Information Protection
2.4 Escalation of the Responsibility of Information Security
2.5 Conclusion

This chapter introduced the concept of information security. The importance of information in relation to the success of modern businesses generally, and IT as an enabler, was discussed. Subsequently, it was emphasised that if information is such a vital component and the IT that drives it is so critical, both should be adequately protected.

The protection of information was then introduced and evidence was produced to show that the need for this protection has existed since before the invention of the modern computer. Information protection, known as information security, defends information against unauthorised disclosure, transfer, modification, or destruction, whether accidental or intentional. It was emphasised that, today, multiple best practices and standards are available to assist organisations in managing information security.

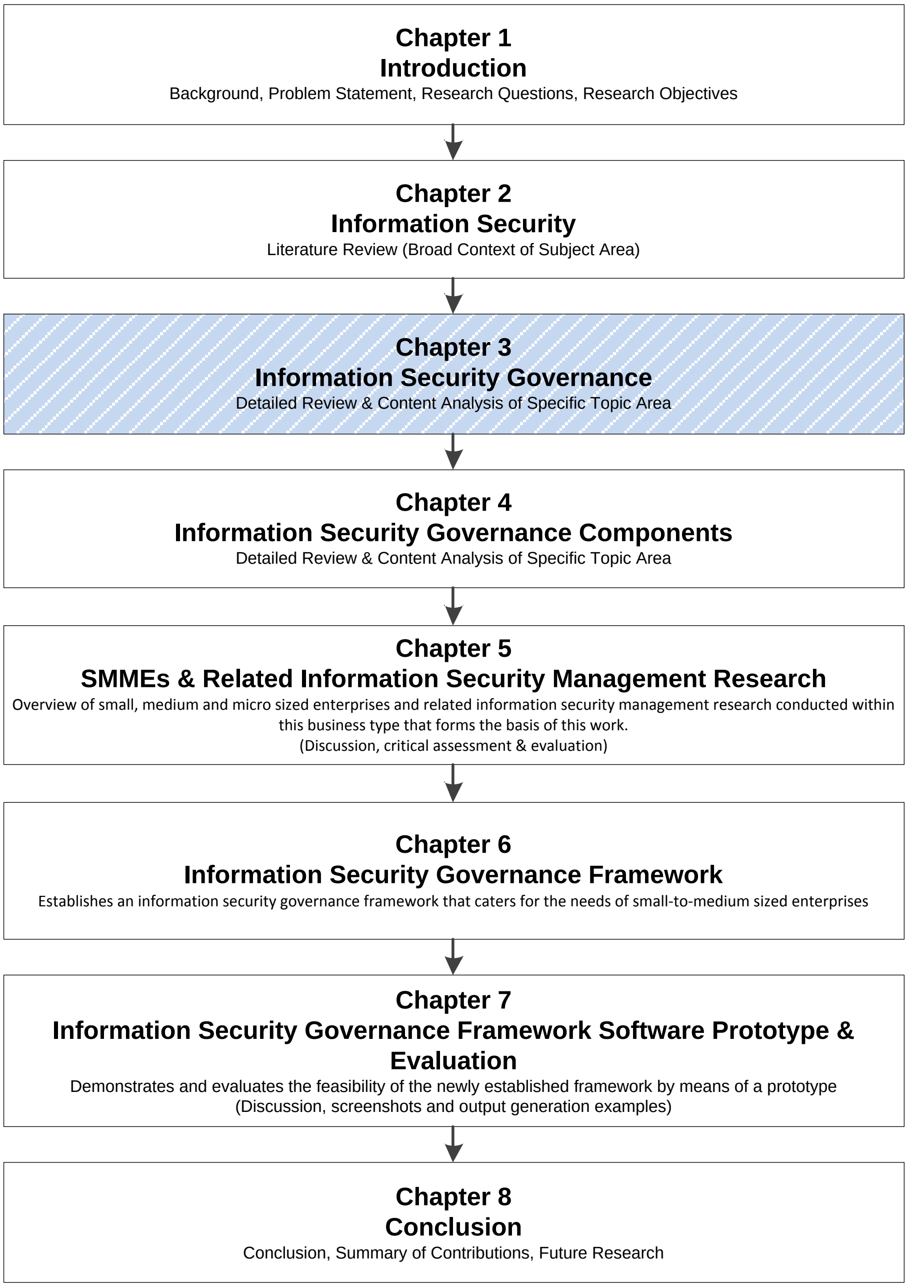
It was further underlined that information, while being transferred, stored and processed using IT, faces many risks. If not countered, these risks were shown to have dire consequences for organisations. Hence, it was argued that a structured process, known as risk management, should be established to mitigate the risks that threaten organisations' information. Risk management entails identifying the risks pertaining to information assets, identifying possible security controls and then applying them to mitigate those identified risks. Three main categories of security controls were shown to exist, namely, physical, logical and administrative controls. Subsequently it was shown that, in order to be effective, the first two categories depend heavily on the third category. The importance of checking compliance and performing regular audits that will ensure continued development and improvement of information security was further emphasised.

The chapter concluded by showing that information security has changed over the years and that the pervasiveness of information has led to the awareness that the responsibility for the proper management and governance of information security lies with executive management. Consequently, if management fails to accept responsibility, the results may be dire and could have the potential to cripple an organisation.

The next chapter will provide a detailed overview of information security governance. It will start by explaining what information security governance is. This will be followed by a discussion on the necessity for executive management to take control of this process, as well as how this can be achieved. It is the intention of this dissertation to use the knowledge gained from this investigation to identify and critically address certain components that are lacking in SMMEs.

Chapter 3: Information Security Governance

This chapter aims to provide an understanding of information security governance by firstly describing corporate governance and thereafter describing IT and information security governance as subcomponents of corporate governance.



Chapter 1
Introduction
Background, Problem Statement, Research Questions, Research Objectives

Chapter 2
Information Security
Literature Review (Broad Context of Subject Area)

Chapter 3
Information Security Governance
Detailed Review & Content Analysis of Specific Topic Area

Chapter 4
Information Security Governance Components
Detailed Review & Content Analysis of Specific Topic Area

Chapter 5
SMMEs & Related Information Security Management Research
Overview of small, medium and micro sized enterprises and related information security management research conducted within this business type that forms the basis of this work.
(Discussion, critical assessment & evaluation)

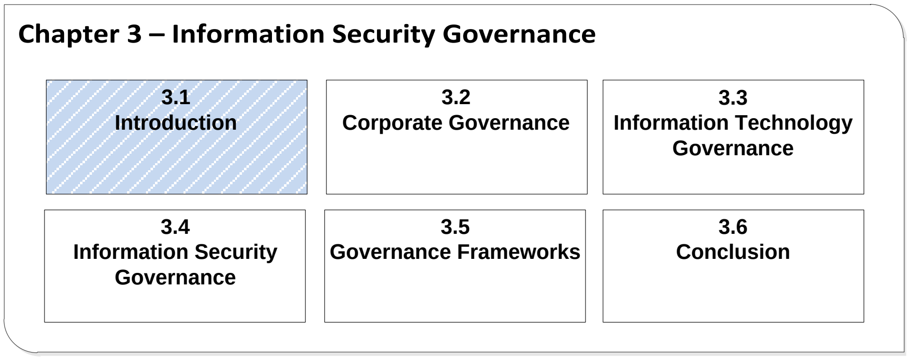
Chapter 6
Information Security Governance Framework
Establishes an information security governance framework that caters for the needs of small-to-medium sized enterprises

Chapter 7
Information Security Governance Framework Software Prototype & Evaluation
Demonstrates and evaluates the feasibility of the newly established framework by means of a prototype
(Discussion, screenshots and output generation examples)

Chapter 8
Conclusion
Conclusion, Summary of Contributions, Future Research

"The complexity and criticality of information security and its governance demand that it be elevated to the highest organizational levels. As a critical resource, information must be treated like any other asset essential to the survival and success of the organization" (Brotby, 2006, p. 1).

3.1 Introduction

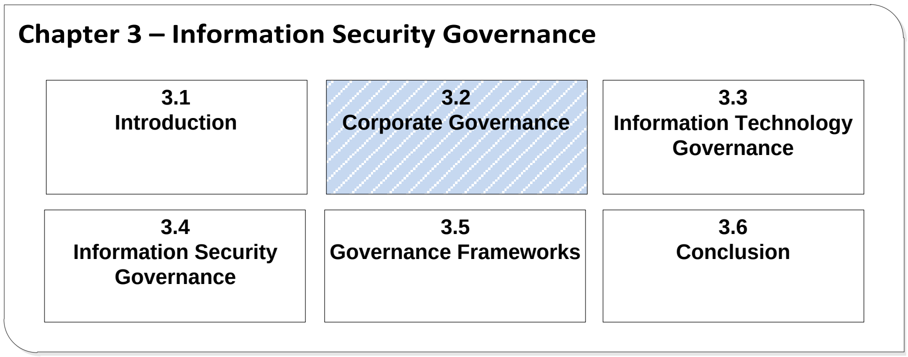

Chapter 3 – Information Security Governance
3.1 Introduction
3.2 Corporate Governance
3.3 Information Technology Governance
3.4 Information Security Governance
3.5 Governance Frameworks
3.6 Conclusion

Information security has transitioned from being seen as a sole technical issue to a modern day business issue that everyone in an organisation has a responsibility to address (S. Von Solms & Von Solms, 2008, p. 139). Furthermore, executive management is increasingly being held accountable for information security, as documented in the information security literature and applicable legislation (Brotby, 2006, p. 7; R. Von Solms & Von Solms, 2006b). As previously mentioned, information is a critical resource and, as a result of its pervasiveness, managing its protection has been elevated to the highest levels of management in the organisation, namely, executive management. The duty of executive management to effectively direct and control information security is generally termed 'information security governance' and forms the primary focus of this work.

Considering that the aim of this work is to establish an information security governance framework, it is essential that an understanding is obtained of what information security governance entails. This should include a definition of information security governance, the reasoning behind its importance to the success of an organisation and, finally, how it can be accomplished.

The topic of information security governance will be detailed in this chapter as follows: Firstly, a discussion on corporate governance is provided to offer a high-level understanding of the governance requirements that should be in place in an organisation. Secondly, two subcomponents of corporate governance, namely IT and information security governance will be discussed, owing to their relevance to information and its protection, which are the focus of this work. Each of these topics will be explained in terms of their definitions, the reasons for their importance and, finally, their implementation. Thirdly, an overview of some existing governance frameworks will be given.

3.2 Corporate Governance

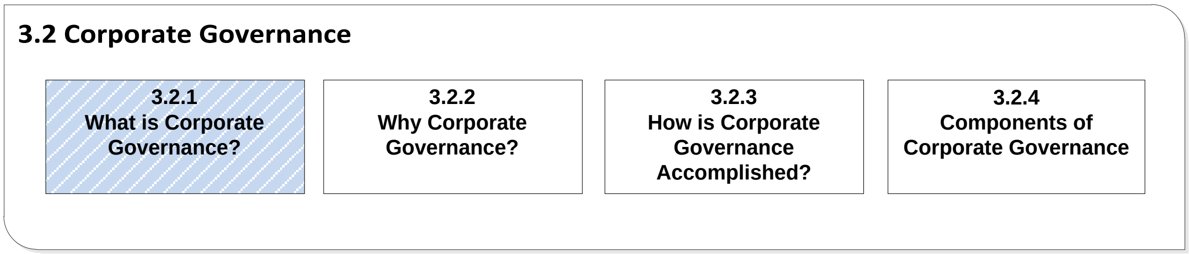


Chapter 3 – Information Security Governance

3.1 Introduction	3.2 Corporate Governance	3.3 Information Technology Governance
3.4 Information Security Governance	3.5 Governance Frameworks	3.6 Conclusion

At the end of the last century, corporate scandals, such as Enron, WorldCom and Tyco, left an undeniable economic aftermath and added vigour to the necessity for corporate governance (Abraham, 2012). Corporate governance involves establishing structures and processes that allow for directing and controlling an organisation (S. Von Solms & Von Solms, 2008, p. 1). The following section will define corporate governance and discuss its importance. Once the importance has been established, the need for IT and information security governance, as part of corporate governance, will be discussed.

3.2.1 What is Corporate Governance?


3.2 Corporate Governance
3.2.1 What is Corporate Governance?
3.2.2 Why Corporate Governance?
3.2.3 How is Corporate Governance Accomplished?
3.2.4 Components of Corporate Governance

There is a common misconception that corporate governance is a new concept. This is, however, not the case, as many of the basic concepts are as old as humanity itself. Debates on the general concepts of governance have been on-going for hundreds of years (Tarantino, 2008, p. 6); nevertheless, corporate governance remains an indefinable term, something similar to love or happiness, of which the essential nature is known, but for which an accurate description cannot be provided (Du Plessis et al., 2011, p. 3). This is as a result of the fact that corporate governance evolves and adapts as each new corporate scandal comes to light and organisations continue to improve their structures and processes (Business Roundtable, 2010, p. 2). Furthermore, cultural differences between countries and jurisdictions also affect governance principles (Du Plessis et al., 2011, p. 18). Despite this, many attempts have been made to provide an explanatory definition for corporate governance.

A general definition of corporate governance entails “the system by which organisations are directed and controlled” (Institute of Directors in Southern Africa, 1994, p. 2). Other definitions introduce other key components of corporate governance:

> Corporate Governance is the set of processes, customs, policies, laws and institutions affecting the way a corporation is directed, administered or controlled (S. Von Solms & Von Solms, 2008, p. 2).
>
> Corporate Governance is to establish executive responsibilities and demand that executive management exercise due diligence in their roles of setting strategy and ensuring that management implements it (Chalaris & Lemos, 2005, p. 60).

> Corporate Governance is used to monitor whether outcomes are in accordance with plans and to motivate the organization to be more fully informed in order to maintain or alter organizational activity. Corporate Governance is the mechanism by which individuals are motivated to align their actual behaviours with the overall participants (S. Von Solms & Von Solms, 2008, p. 2).
>
> Corporate governance is the system of regulating and overseeing corporate conduct and of balancing the interests of all internal stakeholders and other parties who can be affected by the corporation's conduct, in order to ensure responsible behaviour by corporations and to achieve the maximum level of efficiency and profitability for a corporation (Du Plessis et al., 2011, p. 10).

The most important components of corporate governance can therefore be summarised as follows (adapted from Du Plessis et al., 2011, p. 10):

- Corporate governance is the system of directing and controlling an organisation (overseeing).
- Corporate governance is the responsibility of executive management.
- Corporate governance takes into consideration the interests of all parties related to the organisation.
- Corporate governance aims at ensuring responsible behaviour by organisations and its parties.
- Corporate governance ultimately aims to achieve maximum efficiency and profitability for organisations.

Before continuing this discussion on corporate governance, an issue that requires closer analysis is the difference that exists between governance and management of an organisation. A comparison of these two terms is particularly important, as if their differences and relationship are not understood it may lead to confusion.

The Latin origin of the word *governance* denotes steering, and typically includes the exercise of legal and regulatory authority and the use of institutional resources to manage an organisation (Tarantino, 2008, p. 2). The concept of steering, directing and controlling is central to both governance and management in an organisation, but a distinction can still be made on the basis of the organisational level on which they are exercised.

COBIT 5 (ISACA, 2012a) highlights the difference between the management and governance processes by indicating that the two disciplines encompass different types of activity, requiring different organisational structures and serving different purposes. COBIT 5's view on governance is that it "ensures that stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; setting direction through prioritisation and decision making; and monitoring performance and compliance against agreed-on direction and objectives" (ISACA, 2012a, p. 31). By contrast, management "plans, builds, runs and monitors activities in alignment with the direction set by governance to achieve the enterprise objectives" (ISACA, 2012a, p. 31). A distinction can thus be made between governance and management, as shown in Figure 3.1. It should also be noted that these two concepts interact, as governance directs and controls management, while management implements the strategic vision set by governance.

Lazarides and Drimpetas (2008, p. 74) offer a further distinction between management and governance by quoting Professor Robert Tricker as saying, "if management is about running the business, governance is about seeing that it is run properly". Similarly, one can state that governance is concerned with managing the managers in an organisation, thereby emphasising the review component involved. Consequently, it can be concluded that management and governance are intertwined and for an organisation to be successful, both will be required to be present.

Governance not only allows for an organisation to operate successfully, but also offers additional benefits. The potential benefits and justification for corporate governance will become evident from the following subsection.

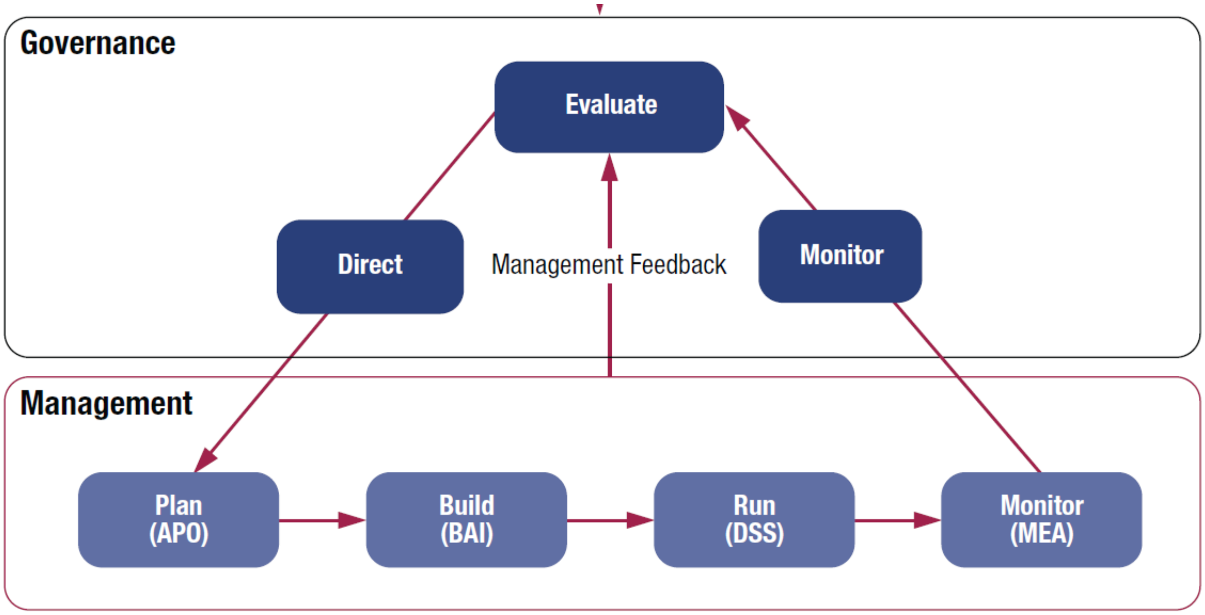


Figure 3.1 – Governance vs. management (ISACA, 2012a, p. 32)

3.2.2 Why Corporate Governance?

3.2 Corporate Governance

3.2.1 **What is Corporate Governance?**	**3.2.2** **Why Corporate Governance?**	**3.2.3** **How is Corporate Governance Accomplished?**	**3.2.4** **Components of Corporate Governance**

There are several reasons why organisations are so interested in corporate governance. Compliance with corporate governance guidelines is often a legal requirement, especially in the United States of America since the promulgation of the Sarbanes Oxley Act (Du Plessis et al., 2011, pp. 304–309). Further, there is a link between sound corporate governance and compliance with the law. Accordingly, governance is not something that exists separately from the law, but rather lifts the bar of what is regarded as appropriate standards of conduct (Institute of Directors in Southern Africa, 2009b, p. 6). Any failure to meet this recognised standard of conduct, albeit not legislated, may render an organisation liable at law (R. Von Solms & Von Solms, 2006b).

Even if corporate governance is not viewed as a legal requirement, there are still many additional benefits that can be obtained from operating an organisation according to sound corporate governance principles and guidelines. One such benefit is an increase in capital investment and customer confidence. Research suggests that organisations following sound corporate governance principles may improve customer confidence, which in turn can add to their corporate success (Organisation for Economic Co-operation and Development, 2004, p. 11). Furthermore, Du Plessis et al. (2011, p. 16) suggest that, in the case of corporations, investors are always willing to pay a higher premium for shares if the organisation is well governed.

The benefits for well-governed organisations are, however, not limited to increased customer confidence and premium stock prices. Research has shown that well-governed organisations may also attract and retain higher levels of talented employment and that their access to capital may be at lower costs compared to poorly governed competitors (Tarantino, 2008, p. 35).

In summary, corporate governance may lead to several benefits that may influence an organisation tremendously, including the following (Tarantino, 2008, p. 36):

- "Greater access to capital markets;
- Lower cost of capital;
- Ability to attract and retain higher-calibre talent;
- Higher-quality and more timely decision making;
- Greater ability to respond to and recover from crises and disasters;
- Improved operational efficiency and lower operating costs;
- Fewer conflicts and lower stress levels; and
- Improved community and industry reputation."

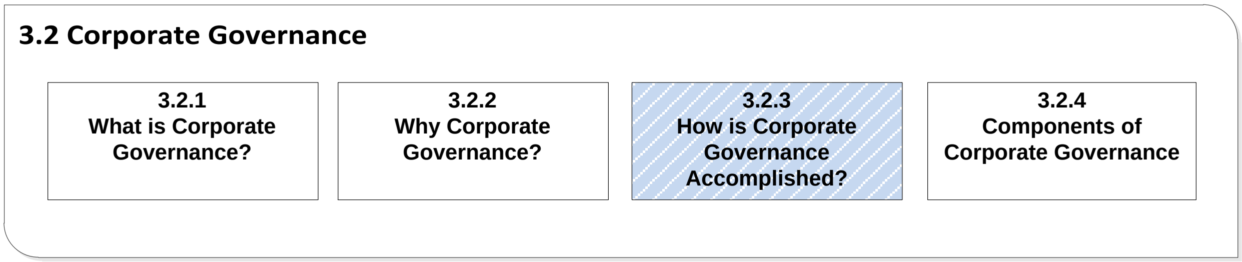
Unfortunately, the converse is also true for poor corporate governance. Organisations should realise that failing to demonstrate sound corporate governance can have adverse consequences. Tarantino (2008, p. 14) demonstrates this by highlighting a few case studies:

- In March 2005, Time Warner, the world's largest media company, paid US$300 million to settle federal fraud charges for overstating its internet subscribers and revenues.
- Similarly, Fannie Mae paid US$400 million in fines to the SEC; its losses totalled US$10,6 billion, shareholder losses totalled US$30 billion, 44 of 55 executives were fired, and 29 were forced to return bonuses.
- Another example is that of former Refco CEO, Phillip Bennett, who was accused of hiding US$430 million in debt in a post-SOX scandal.

As these cases show, organisations may lose billions if corporate governance is not properly addressed. Interest in corporate governance goes beyond that of individual organisations, however. As organisations continue to play a pivotal role in our economies, sound corporate governance is becoming an increasingly important aspect. Countries should be concerned with creating a climate of sound corporate governance since this can make a country "a magnet for global capital" (Institute of Directors in Southern Africa, 2002, pp. 12–14). Conversely, the King Report (Institute of Directors in Southern Africa, 1994, p. 9) indicates that if there is a lack of sound corporate governance in a certain market, capital will promptly leave that market.

This argument clearly supports the importance of corporate governance for organisations and a country's economy. It should therefore not come as a surprise that much work has gone into developing principles and guidelines for corporate governance in this respect.

3.2.3 How is Corporate Governance Accomplished?


3.2 Corporate Governance
3.2.1 What is Corporate Governance?
3.2.2 Why Corporate Governance?
3.2.3 How is Corporate Governance Accomplished?
3.2.4 Components of Corporate Governance

Corporate governance can be accomplished by addressing various managerial principles. In order for each of these principles to be achieved, various management levels within an organisation will need take on certain responsibilities and perform executive tasks accordingly. These tasks may, in turn, be viewed as forming a continuous improvement cycle, which points to the dynamic nature of corporate governance. Each of these components will be discussed in more detail in the following subsections.

3.2.3.1 Principles of Corporate Governance

3.2.3 How is Corporate Governance Accomplished?
3.2.3.1 Principles of Corporate Governance
3.2.3.2 Players in Corporate Governance
3.2.3.3 Dynamic Nature of Corporate Governance

Many countries and institutions have developed codes of practice and guidelines for corporate governance, for example South Africa, the USA and Australia. As corporate governance is a subject area that continues to grow and expand, there is no single code of practice that can be universally applied. In recent years, however, several attempts have been made to identify and explain the ‘essential’ principles of corporate governance (Du Plessis et al., 2011, p. 5).

In the King I (Institute of Directors in Southern Africa, 1994) and II (Institute of Directors in Southern Africa, 2002) Reports, seven essential principles of sound corporate governance were identified:

- Discipline
    - Companies should show an awareness of and commitment to the principles of sound governance, particularly at senior management level.

- Transparency
    - Management should make the necessary information about a company’s financial and non-financial aspects available in a candid, accurate and timely manner.
- Independence
    - Companies should have mechanisms in place to minimise or avoid possible conflicts of interest.
- Accountability
    - Companies should have mechanisms in place to ensure that those who make decisions and take action on specific issues are accountable for their decisions and actions.
- Responsibility
    - Management should behave in a way that allows for corrective action and for penalising mismanagement so as to set the company on the right path.
- Fairness
    - Companies should acknowledge and respect the rights of all groups that have an interest in the company and its future, including minority shareowners.
- Social responsibility
    - Companies should respond to social issues and act in an ethical way.

In the King III Report (Institute of Directors in Southern Africa, 2009a), however, the emphasis shifted slightly with greater emphasis being placed on three additional corporate governance principles:

- leadership
- sustainability
- corporate citizenship.

Firstly, this report stated that corporate governance is essentially about effective, responsible leadership, which it categorised into the following four ethical values:

- Responsibility
    - executive management is responsible for assets and ensuring that the company follows its strategic plan.
- Accountability
    - executive management is accountable to shareholders and other stakeholders.
- Fairness
    - executive management should take account of the interests of all stakeholders when making its decisions.
- Transparency
    - executive management should make comprehensive disclosure of all matters in a clearly understandable manner.

Secondly, it highlights the fact that sustainability is the primary moral and economic imperative of the 21st century. As such, decision makers need to realise that nature, society and business are interconnected and that current incremental approaches to sustainability are not sufficient. Hence, the report indicates that organisations and directors need to change their ways to allow for a fundamental shift in the way they act and organise themselves for sustainability.

Thirdly, the report maintains that the organisation is itself a citizen, or person, which should operate in a sustainable manner. Countries around the world impose responsibilities on citizens; hence, organisations are held accountable in the same manner.

Similar essential principles of sound corporate governance can be found in other published codes of practices for corporate governance. For example, a study of the principles outlined by the Organisation for Economic Co-operation and Development (2004) show similar emphases on transparency and accountability, as well as the other principles and characteristics listed above.

To conclude, it should be realised that corporate governance practices and principles will evolve in response to changing circumstances; accordingly, such principles will be tailored to the circumstances and thus continued change will be experienced. The author of this work therefore supports the statement by Mervyn King that “good corporate governance is a journey and not a destination” (in Du Plessis et al., 2011, p. 11).

3.2.3.2 Players in Corporate Governance

3.2.3 How is Corporate Governance Accomplished?
3.2.3.1 Principles of Corporate Governance
3.2.3.2 Players in Corporate Governance
3.2.3.3 Dynamic Nature of Corporate Governance

A study of the corporate governance codes of practices makes it apparent that there are several players that are widely recognised as being necessary for achieving the previously mentioned principles that establish sound corporate governance. These players may include those working within the organisation itself, the stakeholders and the community (Tarantino, 2008, p. 2). When focusing specifically on those working within the organisation, it becomes clear that all employees are involved (S. Von Solms & Von Solms, 2008, p. 31).

Generally, the employees of an organisation can be divided into three levels, namely (S. Von Solms & Von Solms, 2008, p. 3):

- The strategic level
    - board of directors and/or executive management
- The tactical level
    - senior and middle management
- The operational level
    - lower management and administration.

Taking into account the players in corporate governance, which are mentioned above, as well as the fact that governance and management involves both directing and controlling, the dynamic nature of corporate governance is revealed.

3.2.3.3 Dynamic Nature of Corporate Governance

3.2.3 How is Corporate Governance Accomplished?
3.2.3.1 Principles of Corporate Governance
3.2.3.2 Players in Corporate Governance
3.2.3.3 Dynamic Nature of Corporate Governance

S. Von Solms and Von Solms (2008, pp. 3–4) identify the dynamic nature of corporate governance, shown in Figure 3.2 below, as consisting of two distinct actions: *directing* and *controlling*. This direct–control cycle involves the three levels of management: strategic, tactical and operational.

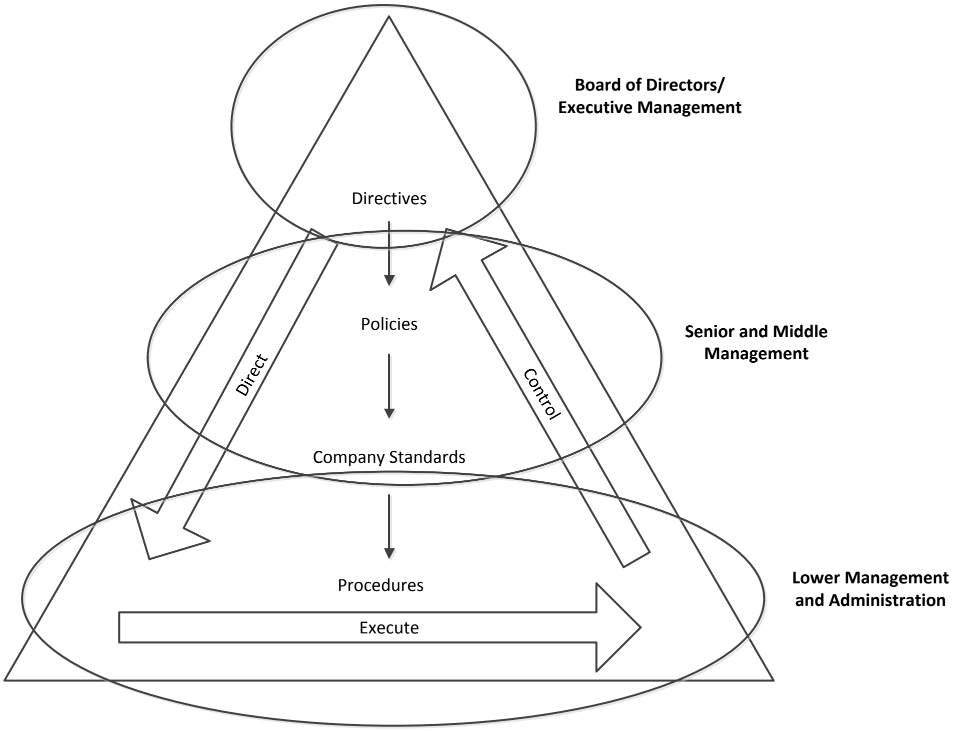


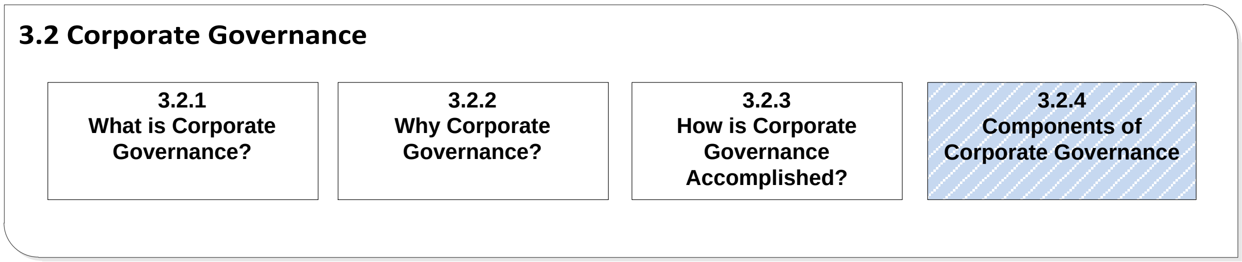
Figure 3.2 – The direct–control cycle (S. Von Solms & Von Solms, 2008, p. 3)

The strategic level is typically formed by the board of directors and/or executive management. In terms of corporate governance, one of the important functions of this level is to provide an organisation with strategic direction, which generally takes the form of directives. Thereafter, the tactical level manages the implementation of the directives received from the strategic management level. This, typically, takes the form of policies, procedures and company standards. Finally, the operational level is responsible for implementing these policies, procedures and standards. Altogether this process represents the direct action of corporate governance (R. Von Solms & Von Solms, 2006a).

By contrast, the control action takes the form of control measures. These control measures are the means by which management monitors (and ensures) that the policies, procedures and standards setting out the direct action are actually complied with (R. Von Solms & Von Solms, 2006a). This is commonly referred to as compliance monitoring and enforcement, which originates from the operational management level, aggregates to the tactical management level and finally to the strategic management level (Coertze et al., 2011).

Corporate governance principles place great emphasis on this direct–control cycle and this will be referred to in subsequent sections. Such emphasis is a result of the fact that the direct–control cycle is also present in the subcomponents of corporate governance.

3.2.4 Components of Corporate Governance


3.2 Corporate Governance
3.2.1 What is Corporate Governance?
3.2.2 Why Corporate Governance?
3.2.3 How is Corporate Governance Accomplished?
3.2.4 Components of Corporate Governance

It is important to realise that corporate governance is accomplished not as a single component, but rather as consisting of various different subcomponents, each covering some part of an organisation’s wellbeing (S. Von Solms & Von Solms, 2008, pp. 7–8). It can therefore be stated that corporate governance consists of a number of ‘sub-governances’, for example:

- financial governance to manage the financial environment
- human resource governance to manage the human resource environment

- IT governance to manage the IT environment.

Figure 3.3 below illustrates this relationship between corporate governance and its subcomponents.

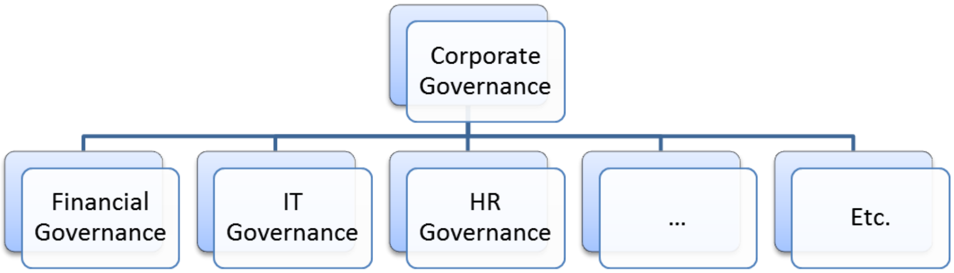
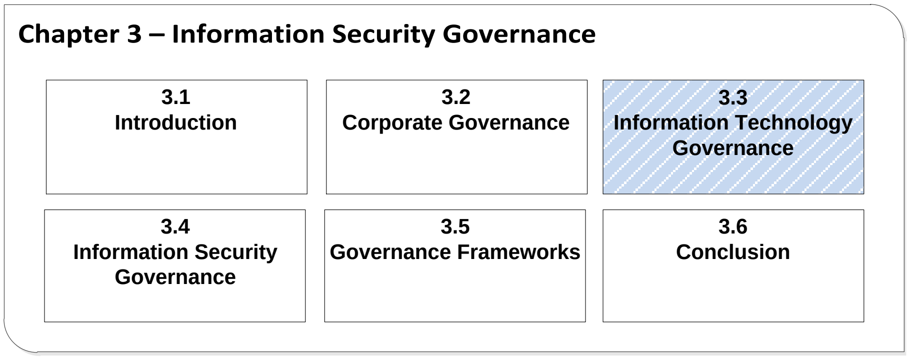


Figure 3.3 – Corporate governance components

(S. Von Solms & Von Solms, 2008, p. 8)

As discussed in this section, corporate governance is an important aspect for executive management to address, since it contributes to organisations meeting their strategic objectives. In view of the importance and value of information as a strategic asset, the governance of IT plays a vital role in meeting those objectives.

3.3 Information Technology Governance



Chapter 3 – Information Security Governance

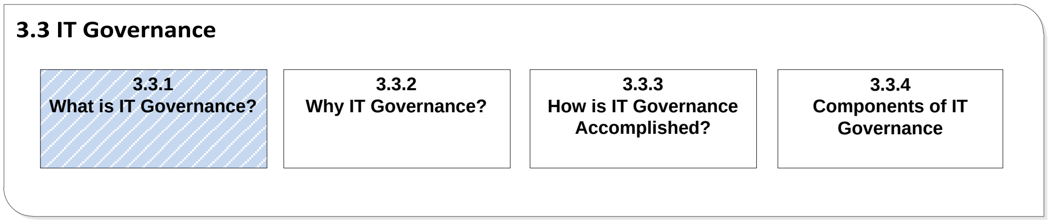
3.1 **Introduction**	**3.2** **Corporate Governance**	**3.3** **Information Technology Governance**
3.4 **Information Security Governance**	**3.5** **Governance Frameworks**	**3.6** **Conclusion**

Information is a critical business asset and continues to be central to nearly all business operations in organisations. Unfortunately, the investments organisations make in order to advance or improve their IT infrastructure have often been disappointing owing to a lack of appraisal and vision by executive management (Devos, Landeghem, &

Deschoolmeester, 2012). For these and other reasons, IT governance has become of critical importance (De Haes & Van Grembergen, 2008).

This section aims to address the relationship between IT and corporate governance. It will discuss the need for IT governance along with what it entails; however, in order to do this IT governance must first be defined.

3.3.1 What is Information Technology Governance?



IT governance, or as it is often referred to, the enterprise governance of IT, is a term that has been evolving rapidly and therefore the literature has provided many definitions over the last few years (Devos et al., 2012).

A general definition of IT governance given by the Institute of Directors in Southern Africa (2009a, p. 119) is “it represents the organisation’s structure and the management of information technology”. Other definitions meanwhile expand on and introduce other components of IT governance.

The ISO/IEC 38500 (2008) standard, dedicated to the governance of information technology, defines information technology governance as the “system by which the current and future use of IT is directed and controlled” (ISO/IEC 38500, 2008, p. 3). Furthermore it “involves evaluating and directing the use of IT to support the organisation and monitoring this use to achieve plans” (ISO/IEC 38500, 2008, p. 3).

Similarly, S. Von Solms and Von Solms (2008, p. 11) define IT governance as “the responsibility of the executive management”. They continue with this definition, saying “it is an integral part of enterprise (corporate) governance and consists of the leadership and organisational structures and processes that ensure that the organisation's IT sustains and extends the organisation's strategies and objectives”.

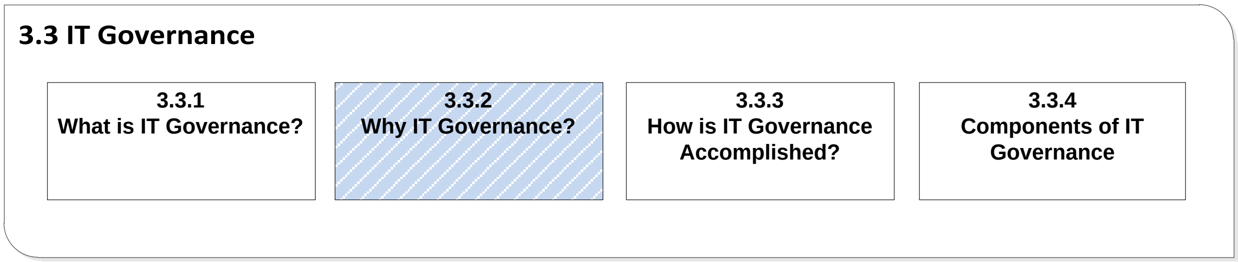
De Heas and Van Grembergen (2009), prominent authors of IT governance literature, define information technology governance as “an integral part of corporate governance and addresses the definition and implementation of processes, structures and relational mechanisms in the organization that enable both business and IT people to execute their responsibilities in support of business/IT alignment and the creation of business value from IT-enabled business investments” (Van Grembergen & De Haes, 2009, p. 3).

The definitions listed above and others from the literature emphasise some of the key principles of IT governance:

- IT governance forms an integral part of corporate governance (S. Von Solms & Von Solms, 2008, p. 11). In order for an organisation to address its corporate governance duties, it must also address IT governance.
- An important component of IT governance entails specifying the structure within which IT decisions will be made and also who will be held accountable (Robinson, 2007);
- The ultimate outcome, or goal, of IT governance is to align the goals of IT with those of the business (Tarantino, 2008, pp. 156–157). IT governance must therefore ensure that it creates value for the organisation by aligning with the organisation’s strategic objectives.
- IT governance involves a set of structures, processes, and mechanisms for making and monitoring IT decisions (Van Grembergen & De Haes, 2009, p. 3). In this context structures include the devices and mechanisms for liaison between business and IT management, processes refer to the strategic IT decision making procedures and finally mechanisms entail the active participation of and collaboration between executives, IT management and business management.

Before considering each of these points in more detail, some reasons why IT governance is viewed as a vital concern in the business world should be highlighted.

3.3.2 Why Information Technology Governance?



The importance of IT governance is closely related to the significance of information in our modern organisations. As previously indicated, the modern business simply cannot exist without information. Today, information is embedded in nearly all business processes and, as such, has been identified as a basic commodity, similar to water and electricity (Drucker, 1993, p. 1). Furthermore, this basic commodity is primarily driven and enabled by IT.

IT has, accordingly, become pervasive in most organisations, and is fundamental to supporting, sustaining and growing the organisation (Institute of Directors in Southern Africa, 2009a, p. 16). Not only is IT a support mechanism, but it is also an important strategic asset that may create opportunities and allow an organisation to gain competitive advantages (Institute of Directors in Southern Africa, 2009b, p. 52). Tremendous advantages have been gained from the emergence and evolution of the internet, e-commerce, online trading and electronic communication (Institute of Directors in Southern Africa, 2009b, p. 15). Organisations thus continue to make significant investments in IT (Lubbe & Jokonya, 2009). Furthermore, virtually all components, aspects and processes of organisations today include some form of automation (Institute of Directors in Southern Africa, 2009b, p. 15). This has resulted in organisations relying immensely on IT.

This high dependence on IT in modern business has resulted in legislation, standards and codes of practice placing great emphasis on IT and its corresponding governance (ISACA, 2012a, p. 13; Institute of Directors in Southern Africa, 2009a, p. 16). Organisations therefore have to address IT governance both as a legal requirement and a best practice.

The five major drivers for IT governance can thus be summarised as follows (Tarantino, 2008, p. 157):

1. “The search for competitive advantage in the dynamically changing information economy through intellectual assets, information, and IT;
2. The rapidly evolving governance requirements, underpinned by capital market and regulatory convergence;
3. The increasing information- and privacy related legislation (compliance);
4. The proliferation of threats to intellectual assets, information, and IT; and
5. The need to align technology projects with strategic organisational goals, ensuring they deliver planned value (project governance)”

These drivers and the aforementioned dependence on IT are thus forcing the executives of today to ask more questions about their IT investments. Such questions include the following (IT Governance Institute, 2008, p. 7):

- “Are we doing the right things?
- Are we doing them the right way?
- Are we getting them done well?
- Are we getting the benefits?”

The IT Governance Institute (2008, p. 10) maintains that these questions can be successfully addressed if IT governance is present in an organisation and is taken seriously by all related parties This is further supported by research that indicates that organisations with effective IT governance may achieve up to 40% better return on their investments (Tarantino, 2008, p. 167). Similarly, organisations with above-average IT governance may show up to 20% higher profits (Tarantino, 2008, p. 167). It should, however, be noted that the benefits of IT governance are not only limited to return on investment and better profits.

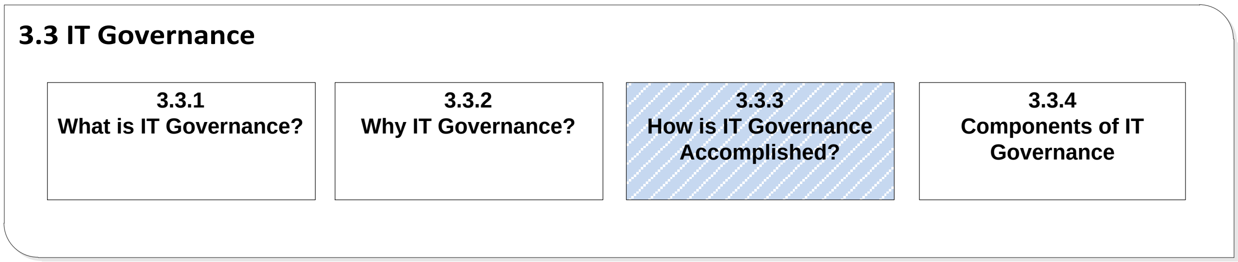
De Haes and Van Grembergen (2008) indicate that additional benefits can also be obtained if IT governance is effectively implemented in an organisation; these include:

- The reputation of the organisation may be improved.
- Trust may be built within the organisation as well as externally.
- Risks in general may be diminished (specifically those related to the IT systems).
- The strategic alignment of IT with the business goals may be achieved, which may lead to competitive advantages (due to reduced costs and increased customer satisfaction).
- Revenue may ultimately be increased.

Unfortunately, the converse is also true in the case of poor IT governance. The Information Technology Governance Institute (ITGI) indicates that “everyday billions are lost or wasted as a result of poor business oversight and decision making regarding information technology investments” (IT Governance Institute, 2008, p. 8). There are many examples of instances where poor IT governance has resulted in huge losses. One example includes the “unauthorised trading by Royal Bank of Scotland (RBS) employees in 2008 that brought the bank to the brink of collapse and resulted in fines of £5,6 million (Financial Services Authority, 2010)” (Coleman & Chatfield, 2011, p. 3). Another example refers to “Marin County (US) and Deloitte in dispute over the perceived failure of an ERP implementation which was attributed to Marin’s apparent lack of organizational and governance maturity, and its inability to absorb business transformation changes associated with this implementation” (Coleman & Chatfield, 2011, p. 3). A more recent example originates from Australia where the “Virgin Blue brand was severely damaged when a computer system failed in September 2010, which severely disrupted flights for 11 days and nearly ended in legal actions being taken against the supplier of the IT system that failed (CIO, 2010)” (Coleman & Chatfield, 2011, p. 3).

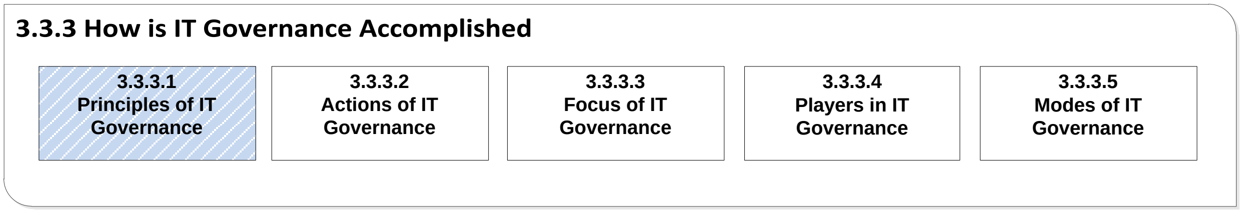
From this argument, it is clear that a lack of proper IT governance is hazardous. Moreover, it may put an organisation at severe risk in the same way as failing to audit its accounts does (IT Governance Institute, 2008, p. 9). Hence, the question that organisations need to ask is not *why* IT governance must be implemented, but rather *how* it can be implemented to achieve prosperity and greater returns on expenditure.

3.3.3 How is Information Technology Governance Accomplished?


3.3 IT Governance
3.3.1 What is IT Governance?
3.3.2 Why IT Governance?
3.3.3 How is IT Governance Accomplished?
3.3.4 Components of IT Governance

IT governance can be accomplished by addressing various managerial principles specifically tailored to IT appraisal. In addition, IT governance requires executive management to perform three distinct actions – directing, controlling and evaluating. These actions, in turn, need to be tailored to the focus areas of IT governance. Unfortunately, executive management is not always educated on these areas of IT governance and may thus require various parties to assist them with their duties. It should, however, be noted that the use of these parties, in addition to the actions of executive management, may be significantly influenced by the degree of dependency that is placed on IT by an organisation. Each of these aspects will be discussed in more detail in the following subsections.

3.3.3.1 Principles of Information Technology Governance


3.3.3 How is IT Governance Accomplished
3.3.3.1 Principles of IT Governance
3.3.3.2 Actions of IT Governance
3.3.3.3 Focus of IT Governance
3.3.3.4 Players in IT Governance
3.3.3.5 Modes of IT Governance

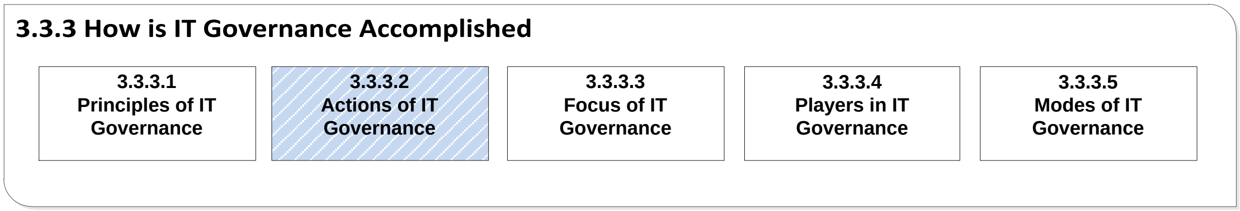
ISO/IEC 38500 (2008) is a high-level, principles-based advisory standard on corporate IT governance. “The objective of this standard is to provide a framework of principles for executive management to use when evaluating, directing and monitoring the use of information technology in their organisations” (ISO/IEC 38500, 2008, p. v). The standard offers six distinct principles in this regard:

1. Responsibility
    - Individuals and groups within the organisation should understand and accept their responsibilities in respect of both the supply of, and demand for, IT.
2. Strategy
    - The organisation’s business strategy should take into account the current and future capabilities of IT; as well as the strategic plans for IT to satisfy the current and ongoing needs of the organisation’s business strategy.

3. Acquisition
    - IT acquisitions should be made for valid reasons on the basis of appropriate and ongoing analysis, and clear and transparent decision making.
4. Performance
    - IT should be fit for purpose in supporting the organisation, providing the services, levels of service and service quality required to meet current and future business requirements.
5. Conformance
    - IT should comply with all mandatory legislation and regulations. Policies and practices should be clearly defined, implemented and enforced.
6. Human behaviour
    - IT policies, practices and decisions should demonstrate respect for human behaviour, including the current and evolving needs of all the people in the process.

In addition to the above-mentioned principles, ISO/IEC 38500 (2008) also highlights that IT governance requires executives to perform or facilitate a series of actions.

3.3.3.2 Actions of Information Technology Governance

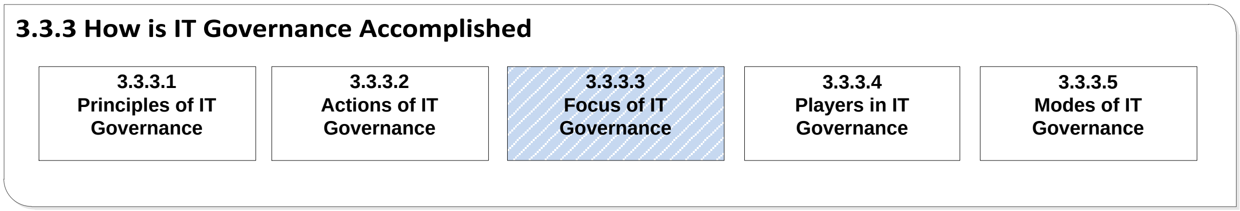

3.3.3 How is IT Governance Accomplished
3.3.3.1 Principles of IT Governance
3.3.3.2 Actions of IT Governance
3.3.3.3 Focus of IT Governance
3.3.3.4 Players in IT Governance
3.3.3.5 Modes of IT Governance

In conjunction with the principles of IT governance previously discussed, the ISO/IEC 38500 (2008) standard states that executives should be in charge of three clear tasks pertaining to IT. These are similar to those mentioned previously for corporate governance (ISO/IEC 38500, 2008, p. 7):

1. *Evaluate* the use of IT.
    - Directors should examine and make judgements on the current and future use of IT, including strategies, proposals and supply arrangements (whether internal, external, or both).
2. *Direct* preparation and implementation of plans and policies.
    - Directors should assign responsibility for, and direct the preparation and implementation of, plans and policies.
3. *Monitor* conformance to those policies and performance against plans.
    - Directors should monitor the performance of IT by means of appropriate measurement systems.

Bearing in mind that executive management should address IT as part of its corporate governance duty and should perform the three previously mentioned actions, the next aspect to consider is what the focus of IT governance is and, hence, what should executive management be addressing.

3.3.3.3 Focus of Information Technology Governance


3.3.3 How is IT Governance Accomplished
3.3.3.1 Principles of IT Governance
3.3.3.2 Actions of IT Governance
3.3.3.3 Focus of IT Governance
3.3.3.4 Players in IT Governance
3.3.3.5 Modes of IT Governance

ISO/IEC 38500 (2008) highlights that executives should perform three actions as part of their IT governance mandate, however the question remains as to what these actions should focus on. Posthumus, Von Solms and King (2010) propose that executive management should focus on five key areas related to IT, which they refer to as the 'penta-bottom line'. These five areas form the focus of IT governance, as shown in Figure 3.4 below (Posthumus et al., 2010):

1. Strategic alignment
   - ensures that the IT investments are aligned with the overall business strategies of the organisation to ensure better returns and increased profits.
2. Resource management
   - ensures that IT has sufficient, competent and efficient resources, both human and equipment, to meet the organisation's demands.
3. Risk management
   - ensures that the organisation assesses IT regularly and reports related risks.
4. Value delivery
   - ensures that actual value is being generated from IT.
5. Performance management
   - encapsulates the concepts of efficiency and effectiveness to ensure accurate, timely and relevant performance of IT management.

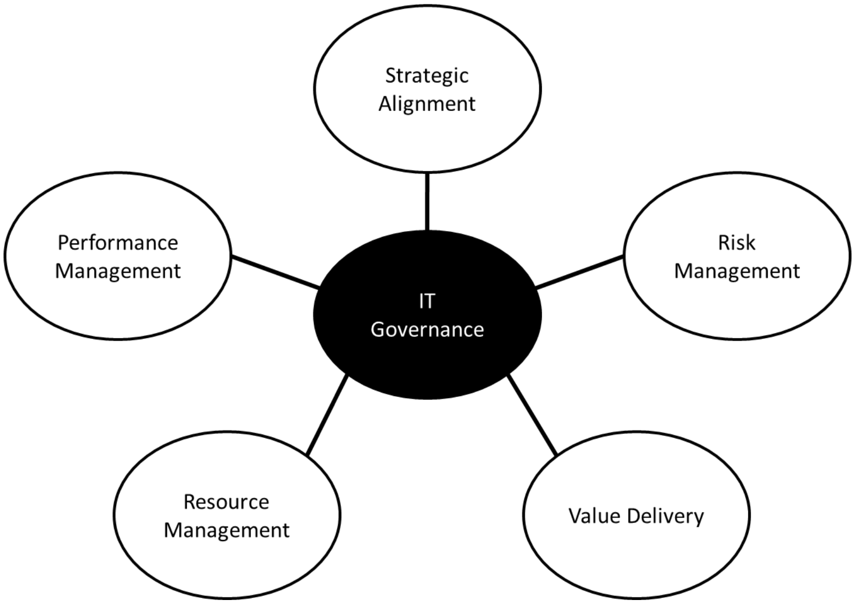
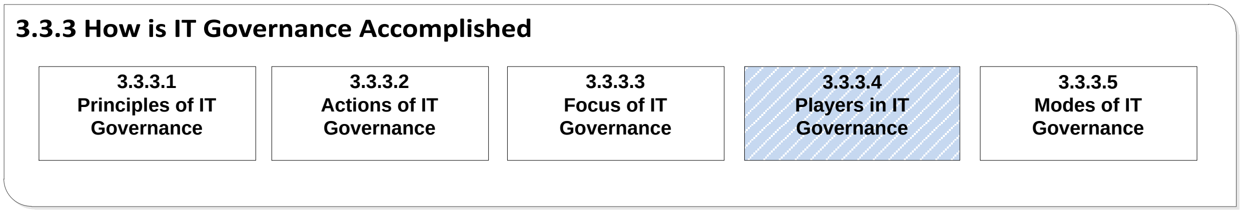


Figure 3.4 – The focus of IT governance (Posthumus et al., 2010)

3.3.3.4 Players in Information Technology Governance


3.3.3 How is IT Governance Accomplished
3.3.3.1 Principles of IT Governance
3.3.3.2 Actions of IT Governance
3.3.3.3 Focus of IT Governance
3.3.3.4 Players in IT Governance
3.3.3.5 Modes of IT Governance

As IT governance is a subcomponent of corporate governance, it should be clear that management in an organisation has a responsibility to address the focus areas previously mentioned.

Butler and Butler (2010) indicate that, owing to the fact that IT governance encompasses such a large number of aspects, as indicated in the previous subsection, all levels of management should pay attention to the IT in an organisation. With reference to corporate governance, three levels of management may be identified in an organisation, namely, strategic, tactical and operational management (S. Von Solms & Von Solms, 2008, p. 3). All three of these management levels have IT governance duties, which are similar to corporate governance. It is, however, important to note that executive management remain ultimately responsible and accountable for the wellbeing of the organisation, including the performance of IT (Institute Of Directors in Southern Africa, 2009a, pp. 70–75).

As executive management may not always be fully aware of or educated regarding IT, they may rely on various committees for assistance and guidance (Institute of Directors in Southern Africa, 2009a, pp. 46–47). Such committees can include the Audit Committee (and Risk Management Committee) and, in some cases, a dedicated IT Oversight Committee (Posthumus et al., 2010).

The Audit Committee is usually responsible for conducting performance reviews of an organisation's system of internal control (Posthumus et al., 2010). It is also responsible for reviewing legal and regulatory compliance efforts, including compliance with organisational rules and codes of conduct (Institute of Directors in Southern Africa, 2009a, pp. 47–62). In many organisations the responsibility for executive IT guidance therefore also falls within the ambit of the Audit Committee.

Additionally, the Risk Management Committee can help executive management to ensure corporate accountability and to address the risks associated with management, assurance and reporting (Institute of Directors in Southern Africa, 2009a, p. 75). In view of the fact that IT poses risks for an organisation, this committee can play a critical role in identifying such risks and reporting them to executive management.

Another possibility is to establish an IT Oversight Committee in an organisation (Institute of Directors in Southern Africa, 2009a, p. 83). The aim of such a committee is to address strategic IT issues in detail, by ensuring that IT is a standard topic on executive management's agenda and that executive management receives all the information it requires in order to make informed decisions (Posthumus et al., 2010).

It is, however, important to note that IT governance should not become the sole responsibility of one of these committees or management levels, but rather a joint responsibility of various parties, with each focusing on a different area (Butler & Butler, 2010), as indicated by Figure 3.5 below.

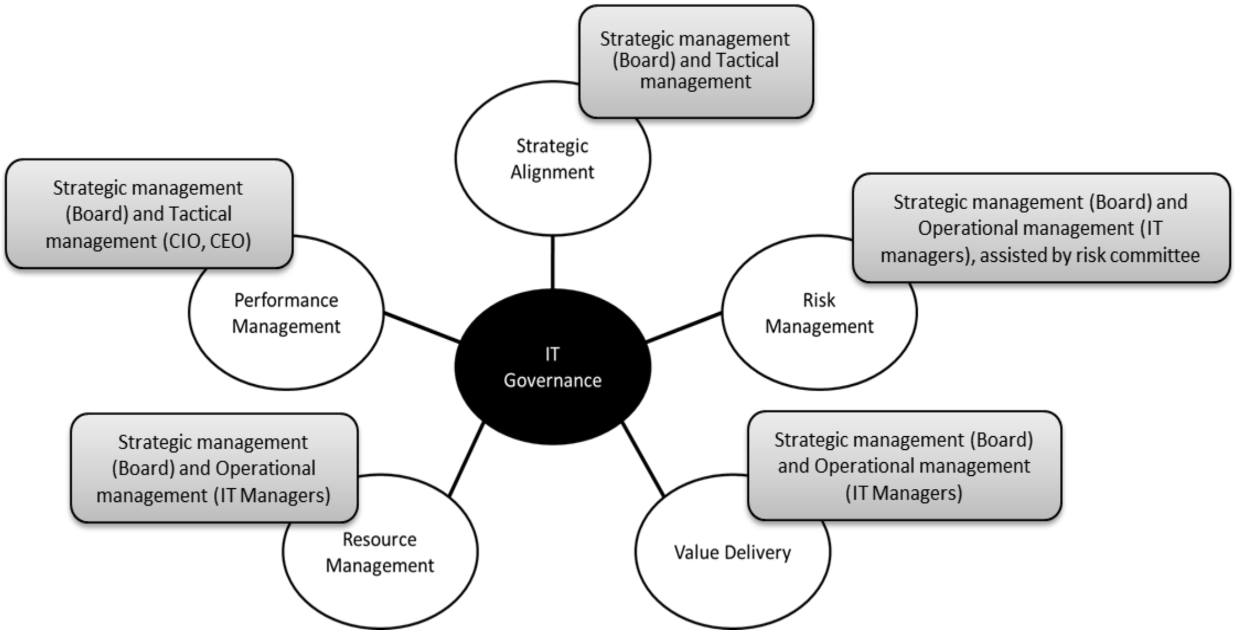
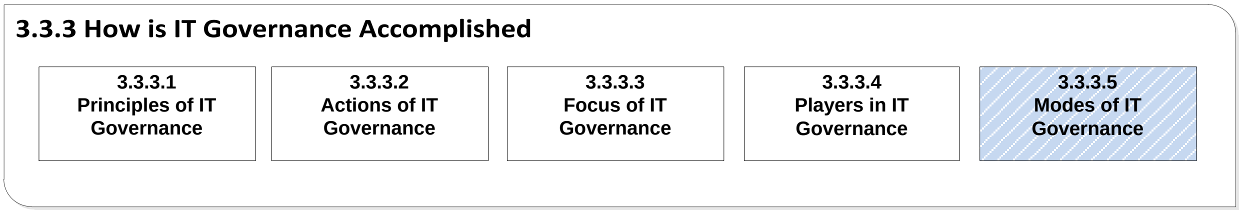

Strategic management (Board) and Tactical management
Strategic Alignment
Strategic management (Board) and Tactical management (CIO, CEO)
Performance Management
Strategic management (Board) and Operational management (IT managers), assisted by risk committee
Risk Management
IT Governance
Strategic management (Board) and Operational management (IT Managers)
Resource Management
Strategic management (Board) and Operational management (IT Managers)
Value Delivery

Figure 3.5 – Players in IT governance (Butler & Butler, 2010)

3.3.3.5 Modes of Information Technology Governance



3.3.3 How is IT Governance Accomplished

3.3.3.1 **Principles of IT Governance**	**3.3.3.2** **Actions of IT Governance**	**3.3.3.3** **Focus of IT Governance**	**3.3.3.4** **Players in IT Governance**	**3.3.3.5** **Modes of IT Governance**

Organisations' approaches to IT governance may differ depending on their business goals. Consequently, the reliance that is placed on IT may be affected by the business strategy, which will subsequently influence the governance of IT.

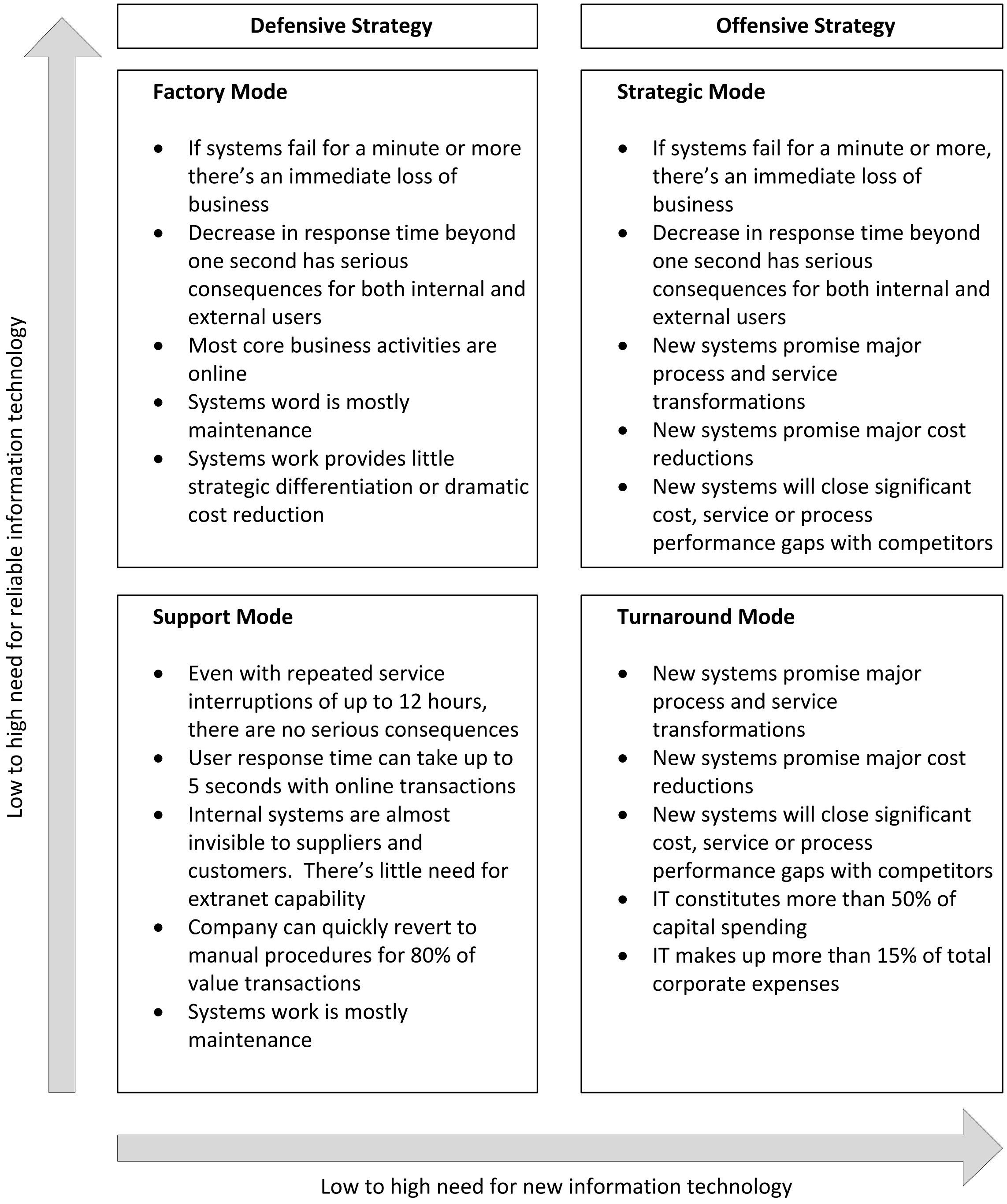
It is vital for organisations to be very clear about their business strategy and, subsequently, to determine how IT will be applied to realise that strategy (Posthumus et al., 2010). Once done, this will assist the organisation in determining its stance towards IT governance and to understand the level of detail that will be needed to implement it. Nolan and McFarlan (2005) offer research that provides considerable insight into the dependency that may exist between an organisation's strategy, or goals, and IT governance.

The IT strategic impact grid (Nolan & McFarlan, 2005), shown in Figure 3.6, indicates that an organisation may apply its IT in terms of two differently defined strategies, namely, a defensive and offensive strategy:

- When IT is used from a defensive viewpoint, the focus is placed on operational reliability; thus, ensuring that the existing IT systems continue to operate and function normally.
- When IT is used with an offensive stance, the focus shifts to strategic issues. This strategy is generally applicable when organisations make use of their IT to gain competitive advantages over their competitors.

Irrespective of whether a strategic or defensive stance is taken, an organisation may adopt a particular mode of IT operation. Such a mode may take on four generally accepted forms, that is, a support, factory, turnaround or strategic mode (Nolan & McFarlan, 2005):

- Organisations in support mode (defensive IT strategy) have a fairly low need for reliable systems and a low need for their IT to be strategic.
- Organisations in factory mode (defensive IT strategy) require dependable systems but it is not essential that they implement cutting-edge technology.
- Organisations in turnaround mode (offensive IT strategy) have technology investments that usually account for more than 50% of capital expenditures and more than 15% of corporate costs.
- Organisations in strategic mode (offensive IT strategy) require the same level of reliability as organisations in factory mode, with the exception that the primary focus shifts to cost reductions and gaining competitive advantages.


Low to high need for reliable information technology
Low to high need for new information technology

Defensive Strategy	Offensive Strategy
Factory Mode • If systems fail for a minute or more there's an immediate loss of business • Decrease in response time beyond one second has serious consequences for both internal and external users • Most core business activities are online • Systems word is mostly maintenance • Systems work provides little strategic differentiation or dramatic cost reduction	**Strategic Mode** • If systems fail for a minute or more, there's an immediate loss of business • Decrease in response time beyond one second has serious consequences for both internal and external users • New systems promise major process and service transformations • New systems promise major cost reductions • New systems will close significant cost, service or process performance gaps with competitors
Support Mode • Even with repeated service interruptions of up to 12 hours, there are no serious consequences • User response time can take up to 5 seconds with online transactions • Internal systems are almost invisible to suppliers and customers. There's little need for extranet capability • Company can quickly revert to manual procedures for 80% of value transactions • Systems work is mostly maintenance	**Turnaround Mode** • New systems promise major process and service transformations • New systems promise major cost reductions • New systems will close significant cost, service or process performance gaps with competitors • IT constitutes more than 50% of capital spending • IT makes up more than 15% of total corporate expenses

Figure 3.6 – IT strategic impact grid (Nolan & McFarlan, 2005)

Posthumus et al. (2010), in referring to the IT strategic impact grid, state that the IT operation modes mentioned previously will influence the different committees that are set up and will affect the frequency with which IT governance is addressed (see Figure 3.7). Organisations following a defensive strategy will generally make use of an audit or risk management committee to report IT matters to executive management every three to twelve months. In some cases an organisation in factory mode may opt to establish and use an IT oversight committee, which may report back to executive management every three months. This may also be the case when an organisation is in factory mode, but places a greater significance on IT for a new business project. Similarly, organisations operating IT with an offensive stance may opt to use such an IT oversight committee because of the heavy dependence placed on IT to gain competitive advantages.

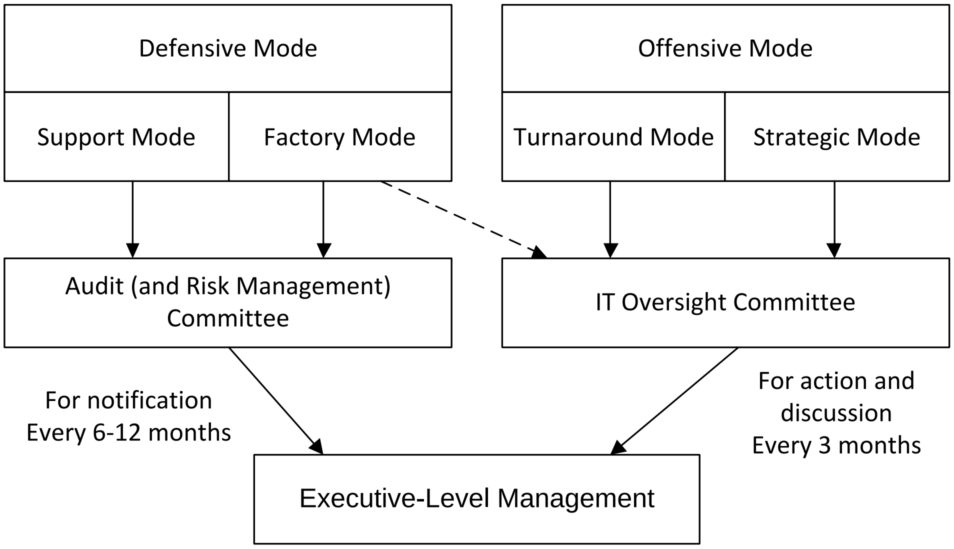
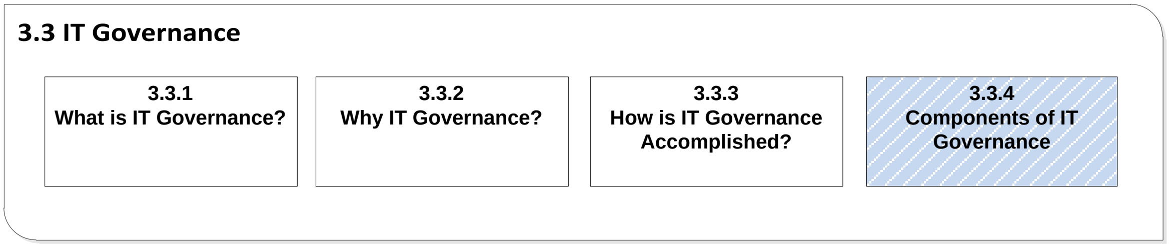


Figure 3.7 – Modes of IT governance (Posthumus et al., 2010)

It can accordingly be concluded that an organisation's business goals will have a direct influence on IT and that the subsequent dependence placed on it will have an impact on the approach used to address IT governance in the organisation. Subsequently, it will also affect the many subcomponents that comprise IT governance.

3.3.4 Components of Information Technology Governance



IT governance is similar to corporate governance in that they both consist of a number of subcomponents. Consequently, IT governance may be perceived as consisting of related types of sub-governance (S. Von Solms & Von Solms, 2008, pp. 17–18), including the following :

- performance and capacity governance
- information security governance.

It is nevertheless important to note that information security governance is not completely encompassed by IT governance. The two concepts should rather be viewed as overlapping components that both fall under the same concept of corporate governance (S. Von Solms & Von Solms, 2008, p. 32), as shown in Figure 3.8. This is in line with the fact that certain aspects of information security governance may be seen as falling outside the domain of IT and its appraisal (Brotby, 2009, p. 50). One example entails the legal and regulatory aspects of information security (S. Von Solms & Von Solms, 2008, p. 32).

The need for IT governance as part of corporate governance has thus been established and its importance identified. It is now important to discuss information security governance as yet another vital component of corporate governance.

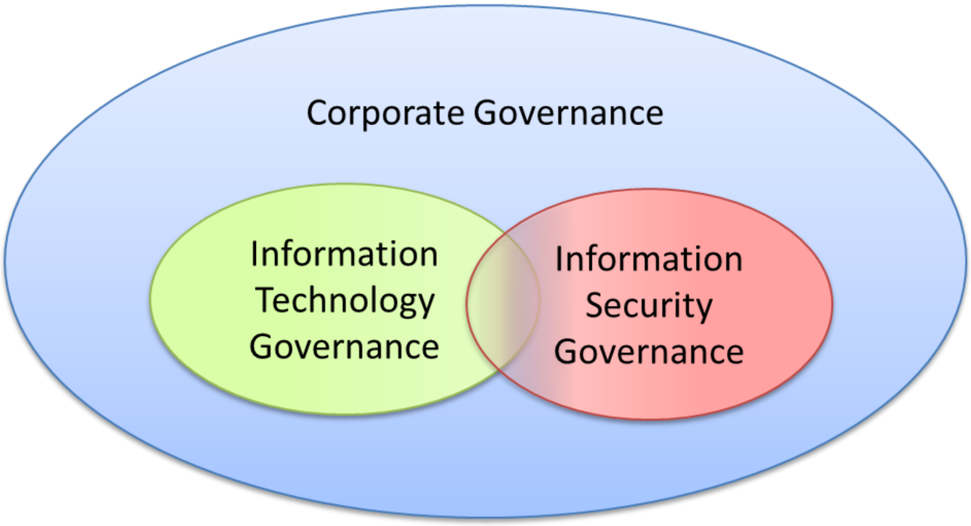
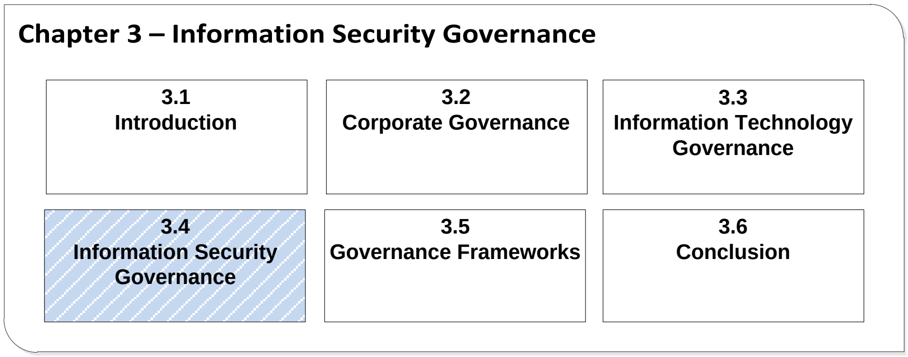

Corporate Governance
Information Technology Governance
Information Security Governance

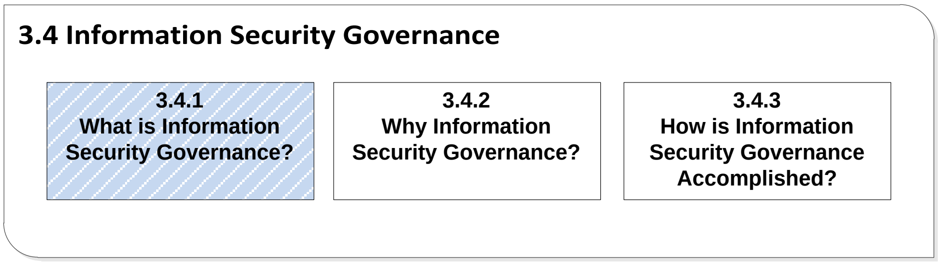
Figure 3.8 – ITG and ISG relationship (S. Von Solms & Von Solms, 2008, p. 32)

3.4 Information Security Governance


Chapter 3 – Information Security Governance
3.1 Introduction
3.2 Corporate Governance
3.3 Information Technology Governance
3.4 Information Security Governance
3.5 Governance Frameworks
3.6 Conclusion

The discussion on information security governance will follow a similar order to that used to discuss corporate and IT governance in this chapter. This section will consider a definition of information security governance and the importance of information security governance. It will conclude by indicating how information security governance can be implemented.

3.4.1 What is Information Security Governance?


3.4 Information Security Governance
3.4.1 What is Information Security Governance?
3.4.2 Why Information Security Governance?
3.4.3 How is Information Security Governance Accomplished?

Information security governance is certainly not a new concept (Pasic, Rodriguez, & Torres, 2008). Many definitions have come into existence over the past few years as it has received more focus and evolved as a result of the collapse of large corporate organisations (Love, Reinhard, Schwab, & Spafford, 2010; Whitman & Mattord, 2012, p. 176).

One general definition of information security governance states that it is “the process of directing and controlling the information security effort by which an organisation protects its information” (Ashenden, 2008, p. 9). It is thus accepted that information security governance entails the directing and control of information security. Unfortunately, this definition does not provide much detail in terms of the responsibility and activities it entails.

Von Solms (2006, p. 167) provides further clarity on this subject by indicating that information security governance is “an integral part of corporate governance, and consists of the management commitment and leadership, organizational structures, user awareness and commitment, policies, procedures, processes, technologies and compliance enforcement mechanisms, all working together to ensure that the protection of the organisations information are maintained at all times”.

From this expanded definition it is clear that information security governance forms part of the corporate governance mandate of an organisation. Executive management, which is ultimately responsible for the wellbeing of the organisation and which performs the corporate governance duty, therefore also has a clear responsibility to review the organisation’s information security effort (S. Von Solms & Von Solms, 2008, p. 139). Nevertheless, despite the fact that the ultimate responsibility for information security remains that of executive management, everyone in the organisation has an important role to play (Von Solms, 2006).

This is further emphasised by considering the several activities that information security governance entails (Hone & Eloff, 2009):

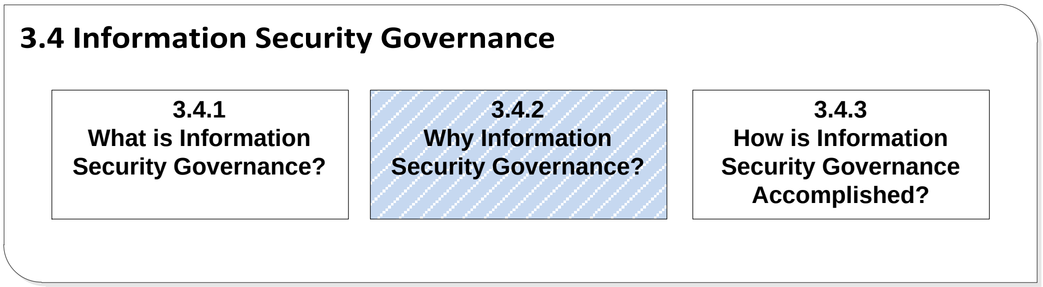
- The identification of the business drivers directing the need for information security within the organisation. This evolves into the definition of the level of security required for the information assets.
- The proactive identification, evaluation and management of threats and vulnerabilities specifically related to the risks associated with the information assets. Both internal and external threats are evaluated.
- The definition of the applicable information security-related governance controls and measures, such as the policies that are required.
- The management and guidance of the stakeholders and role players involved in the information security landscape of the organisation.

- The monitoring of the information security-related controls to ensure that they perform as expected and are adhered to.
- The evaluation of legislation and regulatory requirements and ensuring that the applicable controls are in place to comply with these.

The meaning of information security governance can be further expanded by investigating the clear distinction between it and IT governance (see section 3.3, p. 75). IT governance is primarily focused on the concept of IT, which is by nature technology-centric (Brotby, 2009, p. 2); accordingly IT focuses on the components and elements by which information is stored, processed and transferred. In contrast, information security governance is focused on information security, which goes further in the sense that it is information-centric (Brotby, 2009, p. 2). Hence, it focuses on the true nature and value of information; not just the methods by which it is handled. Information security governance thus takes a much broader view than IT governance, in the sense that it considers many additional components of information which IT does not necessarily cover (S. Von Solms & Von Solms, 2008, p. 32). Information security governance is therefore clearly not just a technical issue, but also a management and governance issue that should be addressed accordingly (Abu-Musa, 2010).

Before considering the implementation details of information security governance, the reasons for its importance should be highlighted in order to provide further insight into its significance in the modern business.

3.4.2 Why Information Security Governance?


3.4 Information Security Governance

3.4.1 What is Information Security Governance?

3.4.2 Why Information Security Governance?

3.4.3 How is Information Security Governance Accomplished?

The significance of information security governance is closely related to the value of information in organisations today. As Benjamin Disraeli stated, “the most successful man in life is the man who has the best information” (Lessing & Von Solms, 2008, p. 1). This statement clearly highlights the importance of information; however, nowadays its protection is equally important.

Some might argue that the primary goal of information security is to protect the information assets of an organisation; however, information is an asset only insofar as it supports the primary purpose of the business, that is, the generation of profits (Brotby, 2008, p. 41). Organisations are thus realising that in order for information security to be truly successful, it has to be aligned to the business goals (Brotby, 2008, p. 19). Information security governance is therefore fast becoming a critical enabler for the realisation of organisations’ business objectives, which, in turn, can result in continued success (Hone & Eloff, 2009).

The significant benefits that are offered by information security governance for continued organisational success include the following (Abu-Musa, 2010; Brotby, 2006, p. 13):

- “An increase in share value for organizations that practice good governance;
- Increased predictability and reduced uncertainty of business operations by lowering information security related risks to definable and acceptable levels;
- Protection from the increasing potential for civil or legal liability as a result of information inaccuracy or the absence of due care;
- The structure and framework to optimize allocation of limited security resources;
- Assurance of effective information security policy and policy compliance;
- A firm foundation for efficient and effective risk management, process improvement, and rapid incident response related to securing information;
- A level of assurance that critical decisions are not based on faulty information; and

- Accountability for safeguarding information during critical business activities, such as mergers and acquisitions, business process recovery, and regulatory response."

These benefits may, in turn, produce significant business returns, on which organisations can capitalise. These include (Abu-Musa, 2010)

- improved internal processes and controls
- potential for lower audit and insurance costs
- improved trust in computer relationships
- protecting the organisation's reputation
- market differentiation through a continuous improvement process, and
- self-governance as a better alternative to regulation.

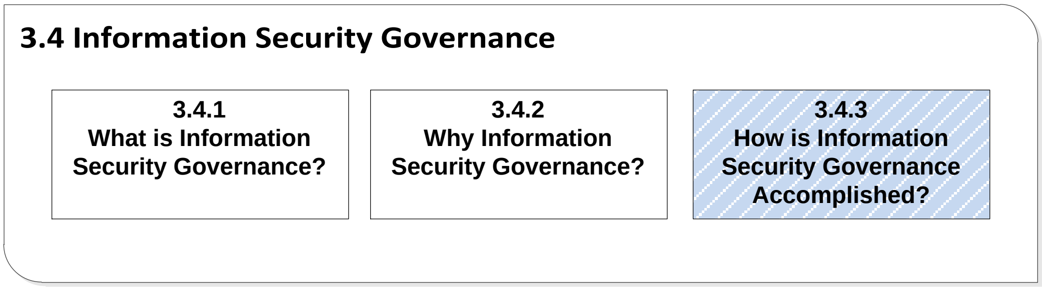
To further highlight the importance of information security governance, it is important to investigate the consequences of poor implementation. Inadequate information security governance may raise severe concerns for an organisation. This is illustrated by Abu-Musa (2010), who offers a list of the consequences that may result from poor information security governance:

- Regulatory actions
    - The loss of data or compromised data integrity could present a serious problem in the confidence of the financial statements or other issues. Noncompliance has multiple penalties that may detrimentally affect the organisation.
- Reputational damage
    - Organisations that experience significant breaches often face a negative reaction from their customers.
- Compromise of competitive advantages
    - The compromise of competitive strategies, pricing, customer and partner information, and other key corporate information can jeopardise an organisation's ability to compete against other organisations that do not make compromises.

- Contractual noncompliance
    - Contracts increasingly contain stipulations for the protection of information. A breach could result in the loss of key contracts, and customers, as well as civil suits.
- Inaccurate or incomplete data
    - Organisations must provide, store and retain accurate and complete information. Inaccurate or incomplete information may result from simple errors to outright fraud. Regardless of the cause, governance efforts should include information integrity.
- Fraud
    - Failure to implement adequate information security will increase the likelihood of successful fraud against the organisation.

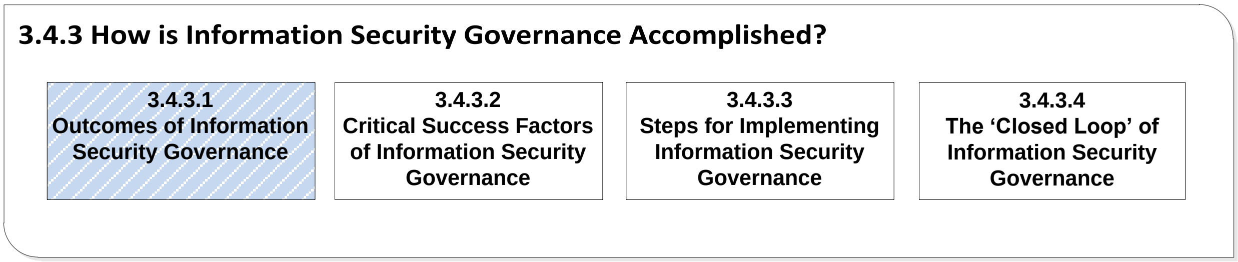
The discussion in this subsection clearly showed that information security governance is gaining importance in the modern business world and, subsequently, that it demands that executive management attends to its duties in this regard. Consequently, a great deal of research has been initiated to gain insight into how information security governance may be accomplished.

3.4.3 How is Information Security Governance Accomplished?


3.4 Information Security Governance
3.4.1 What is Information Security Governance?
3.4.2 Why Information Security Governance?
3.4.3 How is Information Security Governance Accomplished?

Information security governance can be achieved by focusing on a number of characteristics or outcomes. However, before such outcomes can be reached and a successful implementation made, several factors have to be put in place. Once these factors have been addressed the actual implementation of information security governance may commence. This usually takes place in a series of steps. These steps then result in the institution of the direct–control cycle; this forms a ‘closed loop’ originating from executive management and traversing down to operational-level management and administration. This will be discussed in more detail in the following subsections.

3.4.3.1 Outcomes of Information Security Governance

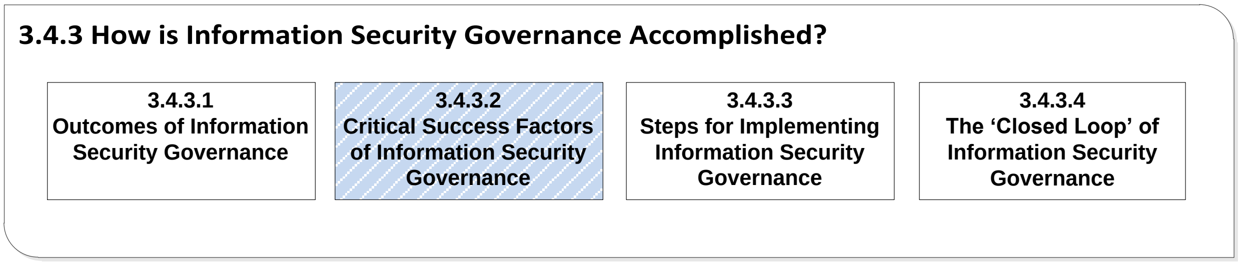

3.4.3 How is Information Security Governance Accomplished?
3.4.3.1 Outcomes of Information Security Governance
3.4.3.2 Critical Success Factors of Information Security Governance
3.4.3.3 Steps for Implementing Information Security Governance
3.4.3.4 The ‘Closed Loop’ of Information Security Governance

Information security governance aims to produce five outcomes, or goals (Brotby, 2009, p. 6; Whitman & Mattord, 2012, pp. 176–177):

1. Strategic alignment
    - ensures that information security is aligned with business strategy to support organisational objectives.
2. Risk management
    - ensures that appropriate measures are put in place to manage and mitigate threats to information resources.
3. Resource management
    - ensures that information security knowledge and infrastructure are applied efficiently and effectively.
4. Performance measurement
    - measures, monitors and reports on information security governance metrics to ensure that organisational objectives are achieved.
5. Value delivery
    - ensures that information security investments are optimised in support of organisational objectives.

These outcomes then are very similar in nature to the focus areas of IT governance (see subsection 0, p. 84), as both information security and IT governance strive for similar outcomes, although the emphasis is on technology and information respectively. It is nevertheless important to realise that these outcomes can only be reached and addressed if certain critical success factors are taken into account.

3.4.3.2 Critical Success Factors of Information Security Governance


3.4.3 How is Information Security Governance Accomplished?
3.4.3.1 Outcomes of Information Security Governance
3.4.3.2 Critical Success Factors of Information Security Governance
3.4.3.3 Steps for Implementing Information Security Governance
3.4.3.4 The 'Closed Loop' of Information Security Governance

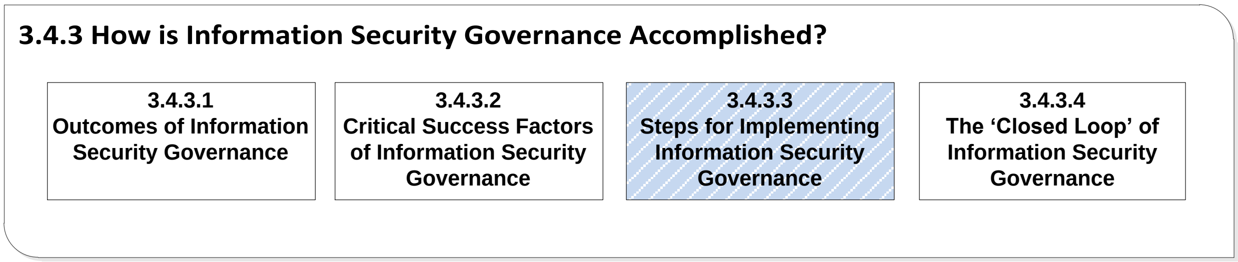
Pironti (2006) indicates that in order for the above-mentioned five outcomes of information security governance to be achieved, that there are six factors that may be viewed as critical to the successful implementation of information security governance in an organisation.

These critical success factors include the following (Pironti, 2006):

- commitment by executive management to information security initiatives
- management understanding of information security issues
- the planning of information security prior to implementation
- the integration of information security with the business
- alignment of information security with organisational objectives
- ownership and accountability for implementing, monitoring and reporting on information security by executives and lower management.

It is thus vital for organisations to ensure that these factors are addressed before attempting to implement information security governance.

3.4.3.3 Steps for Implementing Information Security Governance



3.4.3 How is Information Security Governance Accomplished?

3.4.3.1 Outcomes of Information Security Governance

3.4.3.2 Critical Success Factors of Information Security Governance

3.4.3.3 Steps for Implementing Information Security Governance

3.4.3.4 The ‘Closed Loop’ of Information Security Governance

Once an organisation has taken the necessary precautions to address the critical success factors mentioned, the implementation of information security governance may commence.

S. Von Solms and Von Solms (2008, pp. 157–161) offer fourteen steps (see Figure 3.9) for the successful implementation of information security governance in an organisation:

1. Executive management should recognise that they have a duty in terms of information security and risk management.
2. Best practices for information security and information security governance should be investigated and some should be selected.
3. Risk analysis should be performed and appropriate security controls selected.
4. A corporate information security policy should next be established and signed by the chairman.
5. An information security policy architecture should subsequently be created consisting of a collection of company standards and supporting procedures.
6. Once established, an organisational structure for information security governance should be created.
7. Thereafter, initial compliance/control measures should be implemented and used to report to all three management levels.
8. An awareness programme may also be necessary and this should be implemented to educate employees on their responsibilities and duties.
9. Thereafter the process restarts.
10. Occasional risk analysis may be performed as necessary in order to identify new risks and security control requirements.

11. The information security policy architecture should be kept up to date.
12. Compliance/control measures should be updated to correspond with the policy architecture.
13. Continued awareness-raising should take place regarding information security.
14. A repeating loop then forms between steps 10 to 13.

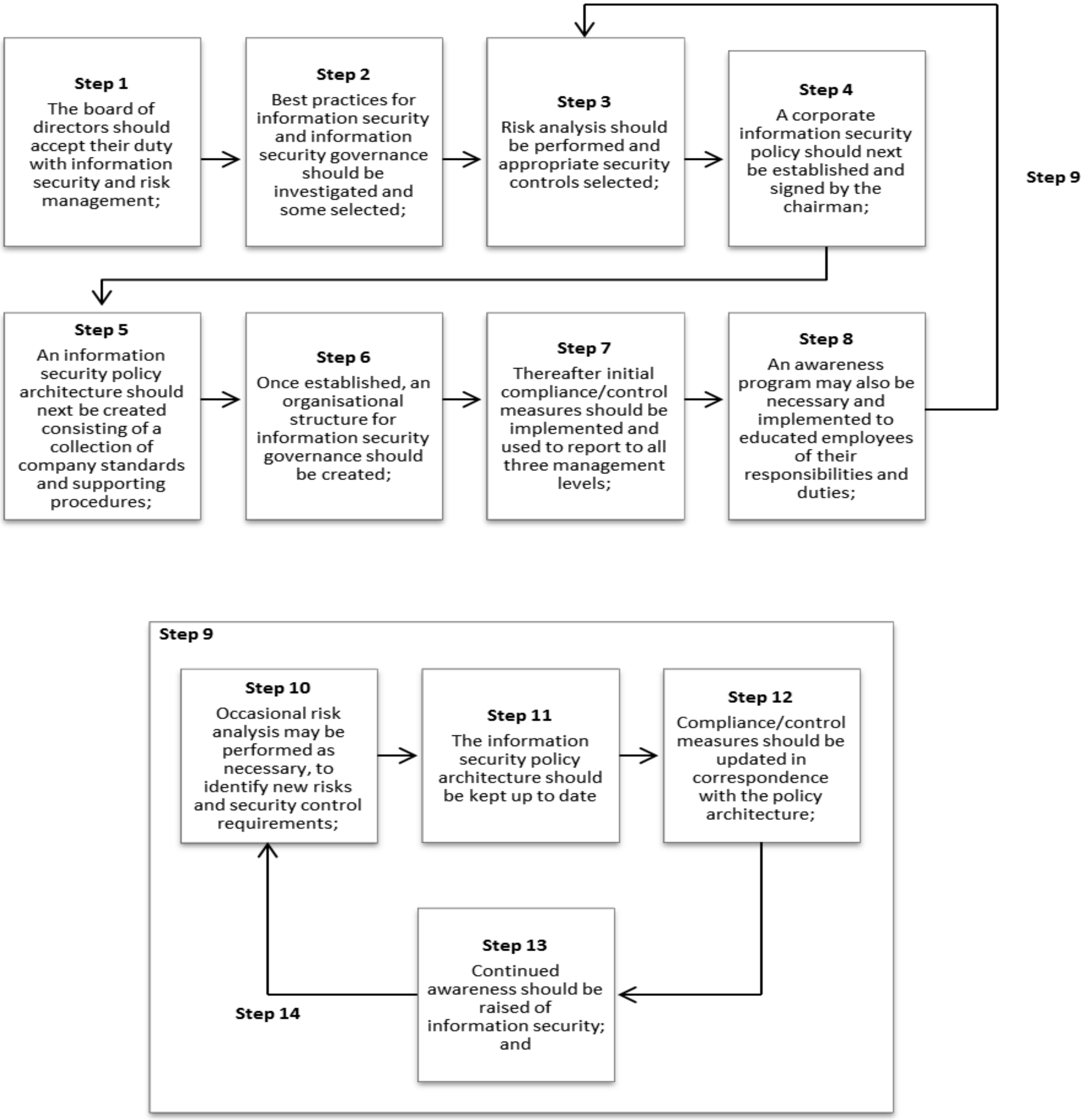
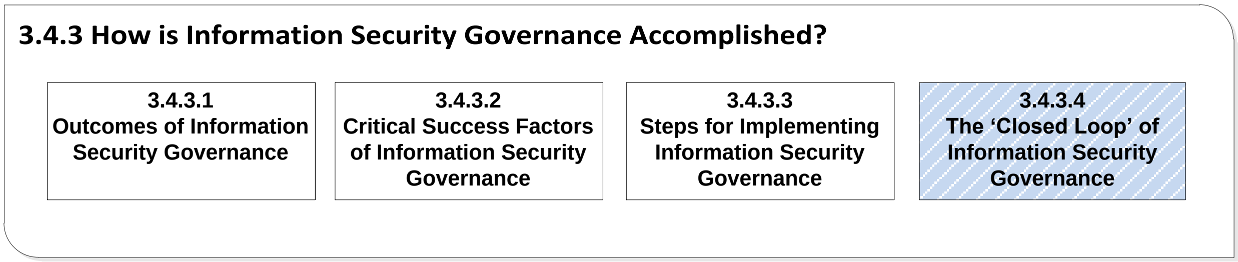

Step 1
The board of directors should accept their duty with information security and risk management;
Step 2
Best practices for information security and information security governance should be investigated and some selected;
Step 3
Risk analysis should be performed and appropriate security controls selected;
Step 4
A corporate information security policy should next be established and signed by the chairman;
Step 9
Step 5
An information security policy architecture should next be created consisting of a collection of company standards and supporting procedures;
Step 6
Once established, an organisational structure for information security governance should be created;
Step 7
Thereafter initial compliance/control measures should be implemented and used to report to all three management levels;
Step 8
An awareness program may also be necessary and implemented to educated employees of their responsibilities and duties;
Step 9
Step 10
Occasional risk analysis may be performed as necessary, to identify new risks and security control requirements;
Step 11
The information security policy architecture should be kept up to date
Step 12
Compliance/control measures should be updated in correspondence with the policy architecture;
Step 13
Continued awareness should be raised of information security; and
Step 14

Figure 3.9 – Steps for ISG Implementation

(S. Von Solms & Von Solms, 2008, pp. 157–158)

3.4.3.4 The ‘Closed Loop’ of Information Security Governance


3.4.3 How is Information Security Governance Accomplished?
3.4.3.1 Outcomes of Information Security Governance
3.4.3.2 Critical Success Factors of Information Security Governance
3.4.3.3 Steps for Implementing Information Security Governance
3.4.3.4 The ‘Closed Loop’ of Information Security Governance

As mentioned, executive management is responsible for providing strategic direction for the organisation and ensuring that the organisation is meeting the set objectives (see subsection 3.2.3.3, p. 73). As has been discussed, this direct–control cycle, affects every level of management in an organisation. Directives are filtered down through all levels of management, who then measure and report on compliance. S. Von Solms and Von Solms (2008, pp. 37–38) explain that this cycle is also true of information security governance.

The loop starts when executive management indicates its commitment to information security by means of board directives (S. Von Solms & Von Solms, 2008, p. 42). These directives state that information security will be treated as a strategic aspect that is pivotal to the existence of the company (S. Von Solms, 2006).

Subsequent to these directives, a corporate information security policy is drafted by tactical-level management and an organisational structure for information security is established (S. Von Solms & Von Solms, 2008, p. 42). Following this, the policy is supported by the many company standards established by tactical-level management, specifying ownership of and responsibilities for information security at all levels (S. Von Solms & Von Solms, 2008, p. 42).

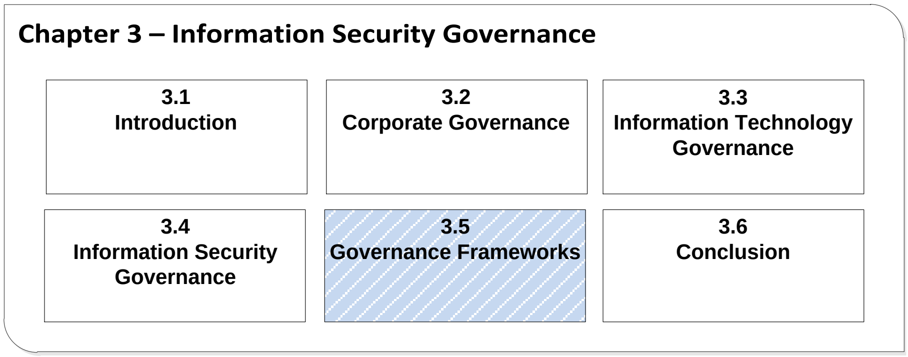
Next, security procedures specific to each company standard are drafted by operational-level management, which provides the operational information that employees should be mindful of when ensuring secure actions (S. Von Solms & Von Solms, 2008, p. 42).

The technology required for this is then rolled out and managed, and compliance monitoring is introduced to measure compliance against procedures and company standards (S. Von Solms, 2006). The results of such compliance monitoring efforts are then fed back to executive management in order to keep them fully informed about the status of information security in the organisation (S. Von Solms & Von Solms, 2008, p. 45). This then closes the loop.

Each of the components mentioned here will receive closer attention in subsequent chapters of this work, as the details of the envisaged information security governance framework are introduced.

A final aspect that requires closer examination is the popular frameworks that may be used for the preparation and implementation of corporate, IT and information security governance. The next section aims to introduce these frameworks while highlighting their importance both to this work and to organisations around the world.

3.5 Governance Frameworks


Chapter 3 – Information Security Governance
3.1 Introduction
3.2 Corporate Governance
3.3 Information Technology Governance
3.4 Information Security Governance
3.5 Governance Frameworks
3.6 Conclusion

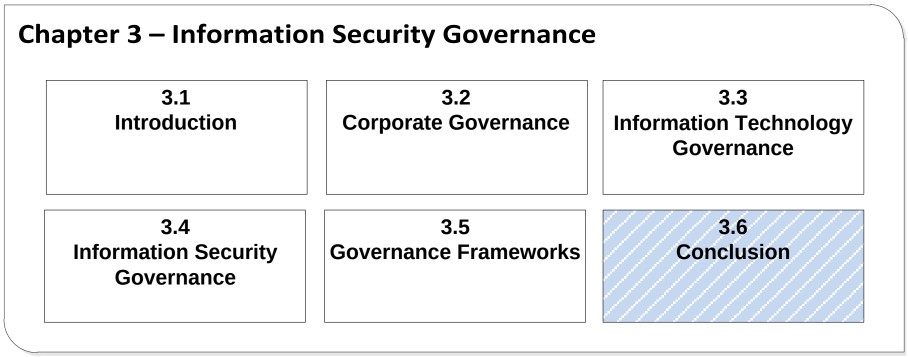
Governance frameworks provide best practices that may be viewed as essential for measuring an organisation's application of sound governance. As a result, successful governance is often related to these frameworks. Earlier in this chapter reference was made to exemplary governance frameworks, including the Institute of Directors in South Africa's *King III Report on Corporate Governance* (2009a) and the Organisation for Economic Co-operation and Development's *Principles of Corporate Governance* (2004), both of which are specifically oriented towards addressing best practices and principles of corporate governance. In support of these, other frameworks are also available that address IT and information security governance.

Two frameworks applicable to IT governance that have gained tremendous attention over the years are the IT Infrastructure Library (ITIL) (Van Bon, 2011) and the Control Objectives for Information and related Technology (CobiT) (ISACA, 2012a). The primary goal of CobiT is to offer guidance to organisations in the form of metrics and maturity models that may be used to determine the achievement of IT goals (IT Governance Institute, 2007, p. 5). CobiT specifically emphasises the importance of closely aligning the business goals of an organisation and IT, as was mentioned earlier in this chapter. Furthermore, CobiT supports the notion that certain aspects of information security and its governance overlap with IT governance (ISACA, 2012a, p. 28). Consequently, CobiT offers some security controls that organisations should implement and address as part of their IT governance implementation. This becomes especially evident when investigating the supplementary material on information security that CobiT offers (ISACA, 2012b), which indicates the close relationship between its objectives and those of well-known information security management frameworks such as ISO/IEC 27001 (2005) and 27002 (2005).

ISO/IEC 27001 (2005) and 27002 (2005), previously discussed in subsection 2.3.2 (p. 40), are both frameworks that offer specific information related to the management of information security in an organisation. Some might argue that these do not address information security governance, but owing to the fact that management is contained within governance they are still applicable in this regard. One example of this is ISO/IEC 27002 (2005), which offers valuable guidance on the duties that the executive management should perform. Executive management, being accountable for information security governance, is therefore addressed by this standard. Similarly, ISO/IEC 27001 (2005) provides specific requirements for the management and auditing, or compliance monitoring, of information security, which also accounts for a large part of information security governance. Consequently, both these two standards may be applicable to the implementation of information security governance in an organisation.

It is thus critical for the modern organisation to adopt such governance frameworks in order to maintain its wellbeing in line with international best practices. This, in turn, may contribute significantly to the organisation's corporate success. As this section indicates, frameworks exist for many types of governance. In terms of information security governance, frameworks emphasise its importance as part of the corporate and IT governance mandate. It is therefore vital that organisations address information security governance accordingly.

3.6 Conclusion



Chapter 3 – Information Security Governance

3.1 Introduction

3.2 Corporate Governance

3.3 Information Technology Governance

3.4 Information Security Governance

3.5 Governance Frameworks

3.6 Conclusion

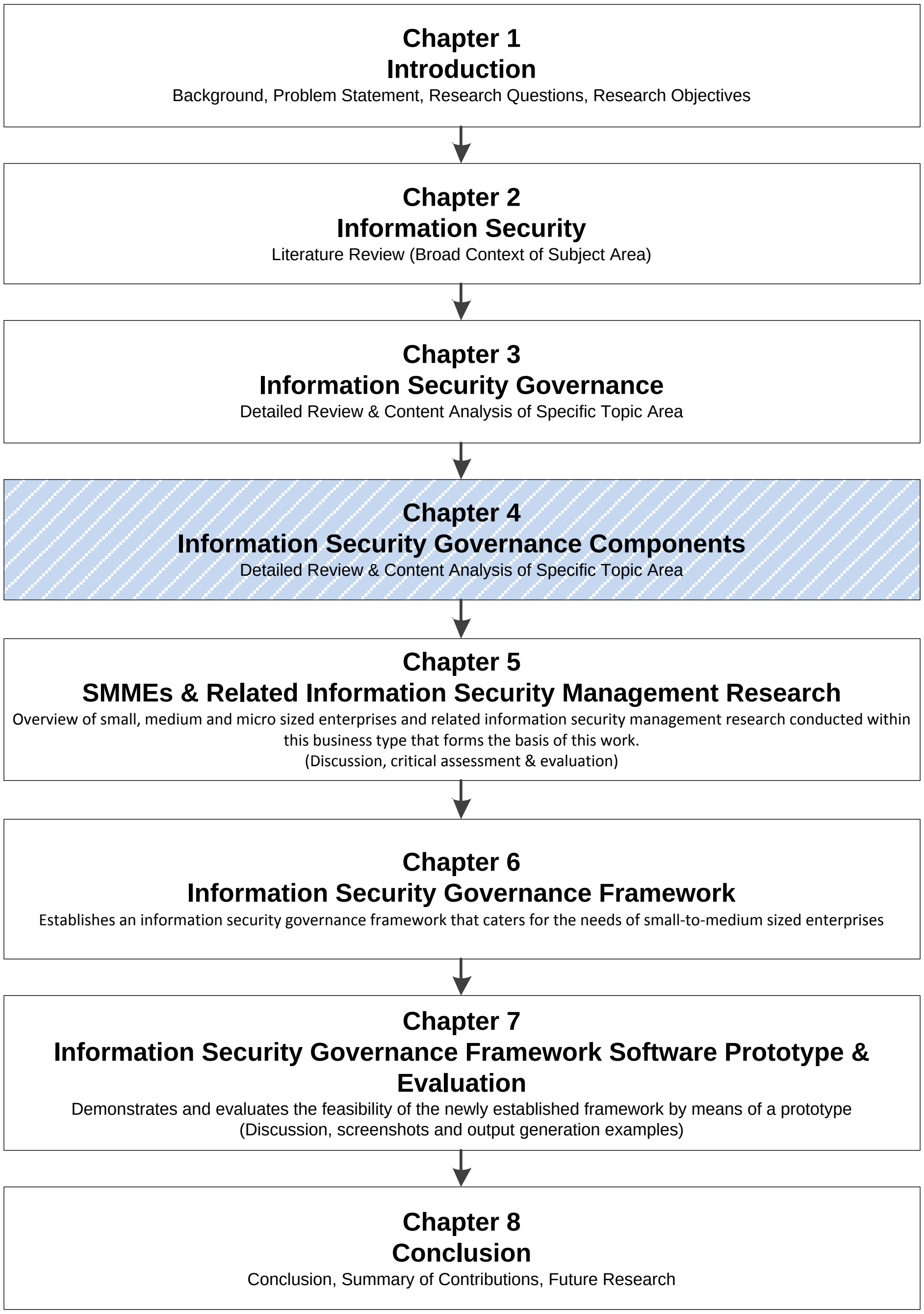
To be able to understand what will be required from an information security governance framework, a sound understanding of what information security governance is, how it is achieved and who will be involved in it is necessary. In this chapter information security governance was described as an integral part of corporate governance. It was further indicated that information security and IT governance are closely related as both influence information and its protection. These two subject areas, corporate governance and IT governance were thus described to ensure a better understanding.

Throughout the chapter, role players in corporate governance, IT governance and information security governance in particular were identified. It was clearly demonstrated that everyone in an organisation should be involved with information security, but executive management remains ultimately accountable. Finally, the requirement for information security governance in all organisations, irrespective of their size, was emphasised.

Furthermore, this chapter mentioned several components, including board directives, policies and compliance monitoring, which assist in the successful implementation and maintenance of information security governance. Considering that the aim of this work is to establish a framework for information security governance, it is essential that these components are discussed in more detail to offer a clear explanation of their necessity and use. A detailed discussion in this regard is thus offered by the following chapter.

Chapter 4: Information Security Governance Components

This chapter aims to investigate in exhaustive detail the components that contribute to successful information security governance implementation.



Chapter 1
Introduction
Background, Problem Statement, Research Questions, Research Objectives

Chapter 2
Information Security
Literature Review (Broad Context of Subject Area)

Chapter 3
Information Security Governance
Detailed Review & Content Analysis of Specific Topic Area

Chapter 4
Information Security Governance Components
Detailed Review & Content Analysis of Specific Topic Area

Chapter 5
SMMEs & Related Information Security Management Research
Overview of small, medium and micro sized enterprises and related information security management research conducted within this business type that forms the basis of this work.
(Discussion, critical assessment & evaluation)

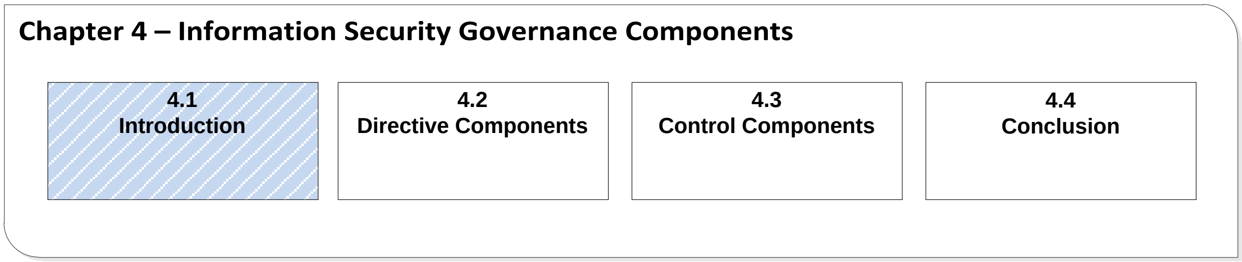
Chapter 6
Information Security Governance Framework
Establishes an information security governance framework that caters for the needs of small-to-medium sized enterprises

Chapter 7
Information Security Governance Framework Software Prototype & Evaluation
Demonstrates and evaluates the feasibility of the newly established framework by means of a prototype
(Discussion, screenshots and output generation examples)

Chapter 8
Conclusion
Conclusion, Summary of Contributions, Future Research

"Many blunder in business through inability or an unwillingness to adopt new ideas. I have seen many a success turn to failure also, because the thought which should be trained on big things is cluttered up with the burdensome detail of little things" – Philip Delaney (Forbes.com, 2012)

4.1 Introduction

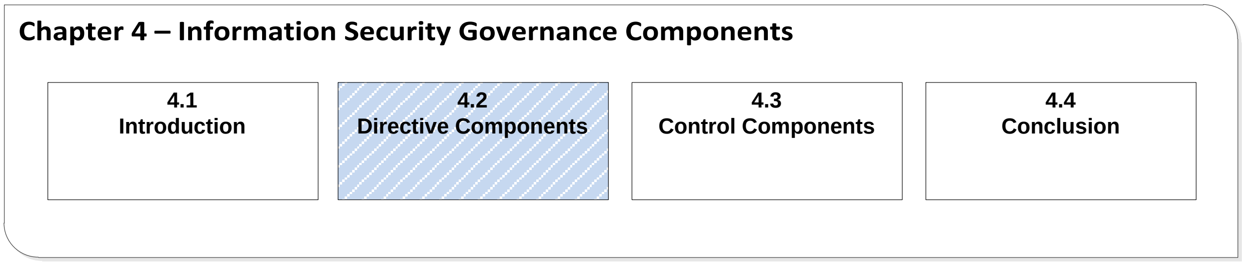


Information security governance is a corporate governance matter that is the responsibility of an organisation's executive management (Brotby, 2006, p. 11). According to the literature on governance, executive management is required to both direct and control information security in order for it to be effective (Brotby, 2009, p. 9; Institute of Directors in Southern Africa, 2009a, pp. 86–87; S. Von Solms & Von Solms, 2008, p. 30). This literature in turn led to the finding, in the previous chapter, that information security governance exhibits a direct–control action cycle (see Figure 3.2, p. 73) that may be identified throughout the management levels in an organisation (S. Von Solms & Von Solms, 2008, pp. 3–4). The previous chapter highlighted several components that assist in the realisation of these two actions, including board directives, policies, procedures and compliance monitoring to name but a few.

Considering that the aim of this work is to establish an information security governance framework, it is essential that a detailed understanding is obtained of the components that contribute to the successful implementation of information security governance.

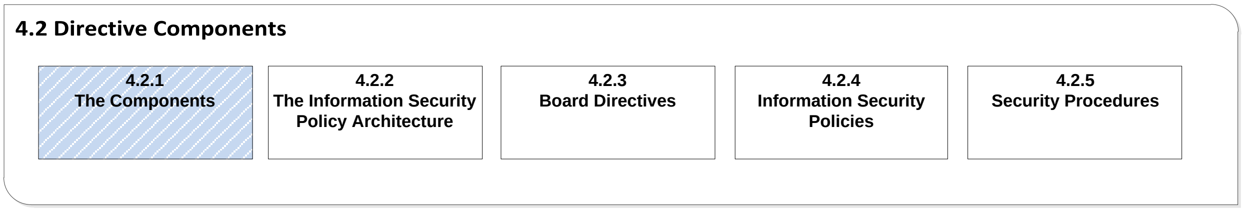
The information security governance components that will be discussed in this chapter are as follows: Firstly, the directive components that support successful information security governance implementation will be deliberated to offer a detailed understanding of the direct action. Secondly, the control components that support monitoring and enforcement of these directive components will be introduced to offer insight into the control action.

4.2 Directive Components



Information security must be properly directed to ensure that it is aligned with the business objectives of an organisation and is truly adding value (S. Von Solms & Von Solms, 2008, p. 41). Information security should add value to an organisation by acting in a supporting role, assisting it to achieve maximum profits and return on investments, rather than becoming a bottomless pit into which money is thrown with no perceptible results (ISACA, 2012b, p. 19). In order to facilitate the above-mentioned supporting role of information security, organisations should address and implement various components, including board directives, policies and procedures, to facilitate the directing of information security (Coertze et al., 2011). This section will thus discuss these components to gain a greater understanding of the direct action exhibited by the direct–control action cycle.

4.2.1 The Components

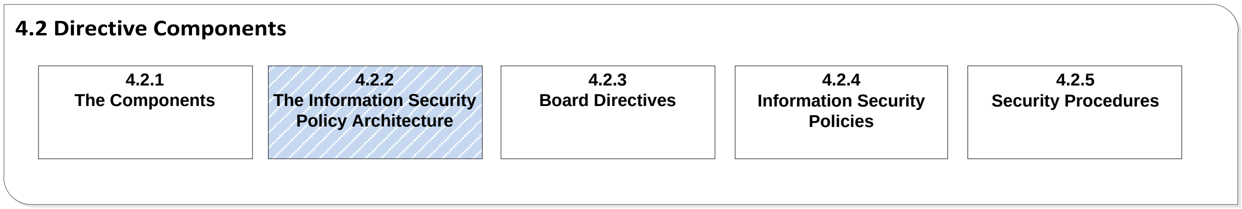


The components that support the directing of information security that will be considered in the rest of this section include the following:

- The board directives that indicate the vision and strategy of the business and which contain specific statements concerning information security governance.
- Information security policies that include
    - the corporate information security policy flowing from the board directives
    - the set of detailed second-level policies flowing from the corporate information security policy
- The set of administrative and operational procedures, again flowing from the detailed set of policies.

All the documents mentioned here work in conjunction with each other to form a hierarchy of directive components, termed the 'information security policy architecture' of an organisation (Bacik, 2008, p. 1).

4.2.2 The Information Security Policy Architecture


4.2 Directive Components
4.2.1 The Components
4.2.2 The Information Security Policy Architecture
4.2.3 Board Directives
4.2.4 Information Security Policies
4.2.5 Security Procedures

The information security policy architecture of an organisation, shown in Figure 4.1, comprises the components, or documents, that facilitate the directing of information security (S. Von Solms & Von Solms, 2008, pp. 74–75).

The information security policy architecture generally enables an organisation to (Bacik, 2008, p. 5):

- "Have a strong commitment to ethics and asset protection;
- Form a benchmark to progress measurements;
- Evaluate how an organisation is doing with its information security program;
- Evaluate how service level agreements are being met through security monitoring;
- Ensure consistency in what the organisation wants to protect;
- Serve as a guide for information security, risk, privacy and compliance; and

- Define acceptable use of organisation assets."

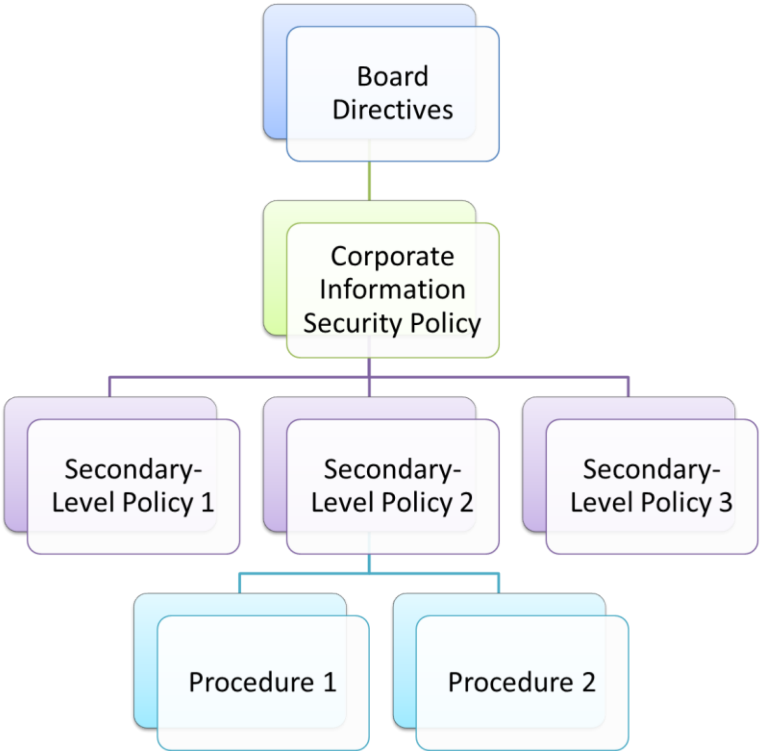


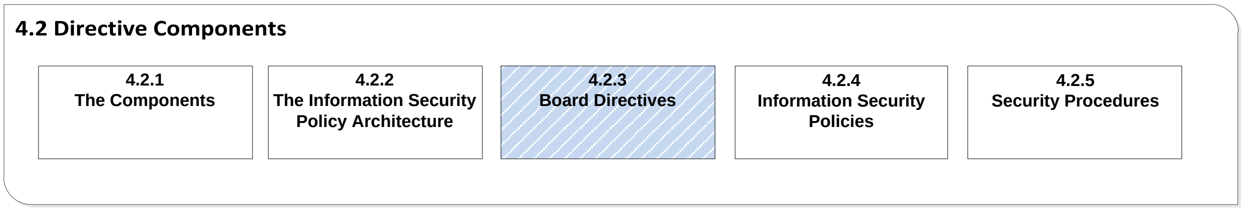
Figure 4.1 – The information security policy architecture

(S. Von Solms & Von Solms, 2008, p. 75)

As illustrated by Figure 4.1, in order to establish an information security policy architecture, executive management first needs to establish board directives. These directives are incorporated and subsequently expanded into a corporate information security policy, usually by the management on the tactical level. This corporate information security policy is, in turn, expanded into multiple secondary-level policies, each of which is further expanded to form administrative and operational procedures at the operational level.

Bacik (2008, p. 6) states that an information security policy architecture can only be successfully implemented in an organisation if those tasked with doing so know the organisation's mission, vision and objectives. This mission, vision and objectives will normally be addressed as part of the board directives (S. Von Solms & Von Solms, 2008, p. 76) and is thus crucial for an information security implementation. It is therefore vital that a clear understanding is obtained as to what board directives entail.

4.2.3 Board Directives


4.2 Directive Components
4.2.1 The Components
4.2.2 The Information Security Policy Architecture
4.2.3 Board Directives
4.2.4 Information Security Policies
4.2.5 Security Procedures

In any organisation it is vital that the board of directors and executive management set the "tone from the top" (Bacik, 2008, p. 13). This entails sharing their strategy, vision and business objectives clearly and concisely with the rest of the organisation, not only for successful business operations, but also for the protection of information assets (S. Von Solms & Von Solms, 2008, p. 42).

Executive management should have a clear vision for the way in which information assets should be handled in terms of protection and access (Bacik, 2008, p. 13). Such a vision will generally be influenced by a number of factors (S. Von Solms & Von Solms, 2008, p. 42):

- external factors, such as legal and regulatory prescriptions and different external risks
- internal factors, such as the strategic vision of the company, the role of IT in the organisation, alignment of IT with organisation strategy, competitiveness, risks from employee behaviour and non-compliance, and so forth.

Once these factors have been considered, executive management will have a clear idea of how important information assets are to the organisation as well as the part they play within the strategic vision. It is this notion that is subsequently captured in board directives (S. Von Solms & Von Solms, 2008, p. 76).

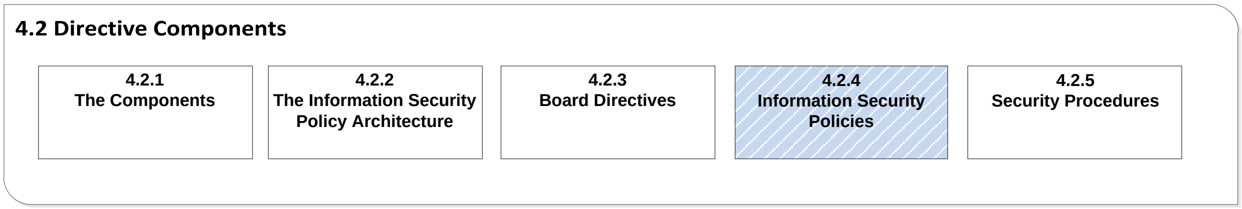
S. Von Solms and Von Solms (2008, p. 76) indicate that board directives reflect the expectations of executive management for information security and other business operations. They continue by mentioning that these directives may appear in many different forms and formats, one example of which is provided below. However, these authors stress that irrespective of the form they take, these directives must show that executive management realises the importance of the organisation's information and information technologies. They should also contain a mandate for the protection of these assets by the rest of the organisation. A mandate in this regard is essential to ensure that a programme for information security implementation will subsequently be initiated.

The following is an example of a board directive. This may be documented or merely communicated verbally during an executive meeting (S. Von Solms & Von Solms, 2008, p. 76):

> The executive management of the organisation realize that the organisation's information technology infrastructure and the information processed by this infrastructure are among the most valuable assets of the organisation.
>
> The protection of these valuable assets is, therefore, of primary importance, and the executive management demand that everybody in the organisation takes responsibility to help protect these assets.
>
> Full support and commitment is given by the executive management to the enforcement of all aspects of information security on corporate level as well as on the level of every individual employee.

Notwithstanding this example, it should be noted that multiple board directives may be established in organisations, which can either expand on an existing directive (such as that given in the example) or focus on a specific area of interest. One such example is information security. Board directives do not necessarily have to address information security only, but they should at least specify a mandate that will motivate and drive future information security implementation efforts (S. Von Solms & Von Solms, 2008, p. 76). These efforts nonetheless require the derived board directives to be interpreted, disseminated and implemented using a series of information security related policies, which offer further detail on how the directives are to be met in the organisation (R. Von Solms, Thomson, & Maninjwa, 2011).

4.2.4 Information Security Policies


4.2 Directive Components
4.2.1 The Components
4.2.2 The Information Security Policy Architecture
4.2.3 Board Directives
4.2.4 Information Security Policies
4.2.5 Security Procedures

Board directives are normally expanded by implementing various information security policies in an organisation (R. Von Solms et al., 2011). “An information security policy includes general statements of rules and applications regulating the liability of employees, security control tools, aims and goals, and management, explaining the protection and distribution of enterprise information entities and the protection of important functions” (Yildirim et al., 2010, p. 1). Policies may differ considerably from organisation to organisation; nevertheless, they remain of critical importance in ensuring that secure practices are maintained (Chipperfield & Furnell, 2010; Yildirim et al., 2010).

Knapp et al. (2009) state that in any organisation policies play an important role, since they provide the blueprint needed to create a platform for secure information practices. These authors continue by highlighting the fact that the ultimate objective of an information security policy is to provide managerial direction and support for information security in line with the business’s requirements and relevant laws and regulations.

Yildirim et al. (2010) elaborate in this regard, stating that policies effectively capture managerial direction and support for information security by means of instructions and actions; these obviously differ from one business to the next. Yildirim et al. (2010) continue by indicating that these instructions and actions would normally be documented by means of general statements, which in turn may include the following:

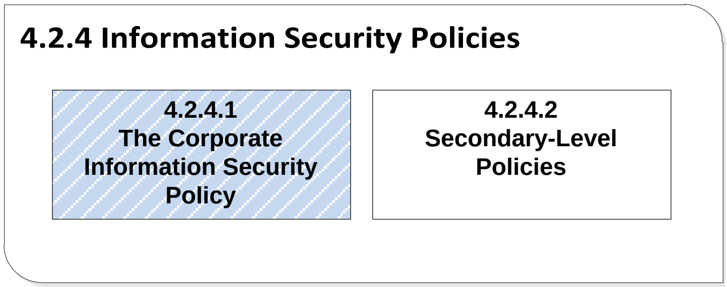
- rules and applications regulating the liability of employees
- the aims and goals, and management of security control tools
- explanations for the protection and distribution of business information entities

- the protection of important functions.

Further, the degree of detail in these general statements and instructions may vary greatly, depending on the type of policy and the audience being targeted.

Different types of information security policies may be present in an organisation, each type being drafted at a specific managerial level and in a certain degree of detail (Bacik, 2008, pp. 47–58). An example of such a policy is the high-level document flowing from the board directives that should be sanctioned by strategic-level management. This policy is termed the 'corporate information security policy' and all related lower-level information security documents flow from this (S. Von Solms & Von Solms, 2008, p. 77).

4.2.4.1 The Corporate Information Security Policy


4.2.4 Information Security Policies
4.2.4.1 The Corporate Information Security Policy
4.2.4.2 Secondary-Level Policies

Organisations may call their corporate information security policies by different names, as among others, a general security policy, an organisational security policy, an enterprise information security policy, an IT security policy, and an information security policy (R. Von Solms et al., 2011). Irrespective of the term used, international standards and best practices dictate that it must exist (Information Security Forum, 2007; ISACA, 2012a, pp. 67–68; ISO/IEC 27001, 2005, p. 13; ISO/IEC 27002, 2005, p. 7). In view of the fact that a foundation must be established for information security, as well as the recommendations and requirements mentioned, this type of policy is often one of the first to be drafted in an organisation (Bacik, 2008, p. 47).

A corporate information security policy constitutes "an official executive document, which directly supports the board directives of an organisation and that sets the strategic direction, scope and tone for information security implementation" (Whitman &

Mattord, 2012, p. 180). Such a policy will usually form the pinnacle of the information security policy architecture, as it becomes the source from which all other policy documents are derived (Bacik, 2008, p. 97).

Consequently, Whitman and Mattord (2012, p. 180) indicate that a corporate information security policy typically guides the development, implementation and management of information security, as it defines the purpose, scope, constraints and applicability of information security in an organisation, as well as assigning responsibilities for the various areas of security to related parties. It therefore sets out the requirements that must be met by information security in an organisation (Knapp et al., 2009).

Although the specifics of this policy may vary from organisation to organisation, it normally includes the following elements (Whitman & Mattord, 2012, p. 180):

- “An overview of the corporate philosophy on security;
- Information on the structure of the information security organization and individuals who fulfil the information security role;
- Fully articulated responsibilities for security that are shared by all members of the organization (employees, contractors, consultants, partners, and visitors); and
- Fully articulated responsibilities for security that are unique to each role within the organization.”

Also of great importance to this work and this policy is clause 5 of ISO 27002 (2005), which provide definitive directives on what this policy should include. In support of this, S. Von Solms and Von Solms (2008, p. 77) also recommend that specific guidelines should be followed in order to draft a sound corporate information security policy. These guidelines, which may also be viewed as adding to the definition and satisfying the directives of ISO 27002 (2005), include that such a policy should:

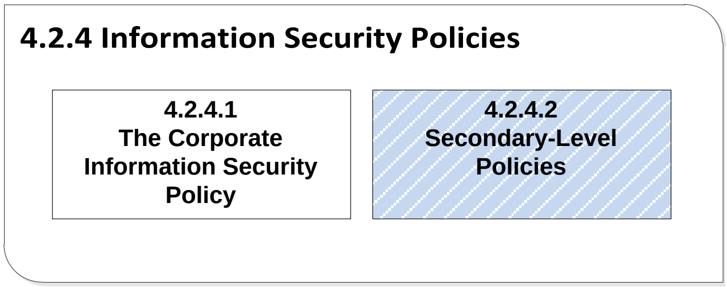
- indicate executive management commitment and clearly flow from higher-level directives
- be accepted and signed by a high ranking officer

- not be a long document, nor should it be written in technical language. The maximum length should be about four to five pages, and it should contain high-level statements concerning information security.
- not change very often, and should be ‘stable’ as far as technical developments and changes are concerned
- not contain any references to specific technologies, and should be ‘technology neutral’
- indicate who the owner of the policy is, and what the responsibilities of other relevant people are
- indicate the scope of the policy, that is, all the people who will be subject to the policy
- refer to possible (disciplinary) actions for non-conformance, as well as lower-level constituent policies or company standards
- be distributed as widely as possible in the organisation, and should be covered in all relevant awareness courses.

A sample corporate information security policy which satisfies most of the points mentioned above has been added to the end of this work as Addendum A, p. 222.

From the discussion above, it is thus evident that business strategy, or board directives, drive the drafting and content of a corporate information security policy and, subsequently, the implementation of information security. It is, however, important to note that this policy is usually drafted at a very high level of abstraction with little reference made to the way in which adherence and implementation should take place in the organisation; consequently, it too needs to be expanded to offer fuller comprehension (R. Von Solms et al., 2011). This is generally achieved by drafting secondary-level policies (S. Von Solms & Von Solms, 2008, pp. 82–83).

4.2.4.2 Secondary-Level Policies


4.2.4 Information Security Policies
4.2.4.1 The Corporate Information Security Policy
4.2.4.2 Secondary-Level Policies

The directive components, board directives and corporate information security policy mentioned in the previous section will generally be sanctioned by strategic-level management and will detail the vision and intent for information security in the organisation (R. Von Solms & Von Solms, 2006a). Regrettably, these components offer little detail as they often contain only high-level statements (S. Von Solms & Von Solms, 2008, p. 83). This is especially true of a corporate information security policy, which normally indicates what must be done insofar as information security implementation and adherence is concerned, but offers little in terms of how this should be organised (Grobler & Von Solms, 2004). Consequently, this policy needs to be supported by various secondary-level policies which should be drafted by tactical-level management (R. Von Solms et al., 2011). Generally, secondary-level policies manifest in two different types, namely, company standards and issue-specific policies (S. Von Solms & Von Solms, 2008, p. 83).

A company standard, as a type of secondary-level policy, is a written document that consists of a set of accepted rules that provides detailed instructions on the use of an organisation’s processes, technologies and systems (R. Von Solms et al., 2011). A company standard will generally define specific aspects of the corporate information security policy in more detail (S. Von Solms & Von Solms, 2008, p. 83).

Furthermore, a company standard typically specifies the specific security controls that will be implemented and operated in an organisation to ensure that a specific security risk is addressed (Coertze et al., 2011). Accordingly, company standards offer specific details on the way information security will be implemented in the organisation, as well as forming an essential foundation for monitoring policy compliance and adherence (Brotby, 2009, p. 116).

This type of secondary-level policy is thus referred to as a company standard, owing to the fact that it can be viewed as a standard, or benchmark, against which the adequacy of information protection will be measured in an organisation (BusinessDictionary.com, 2012). A sample company standard may be viewed within Addendum B, p. 228.

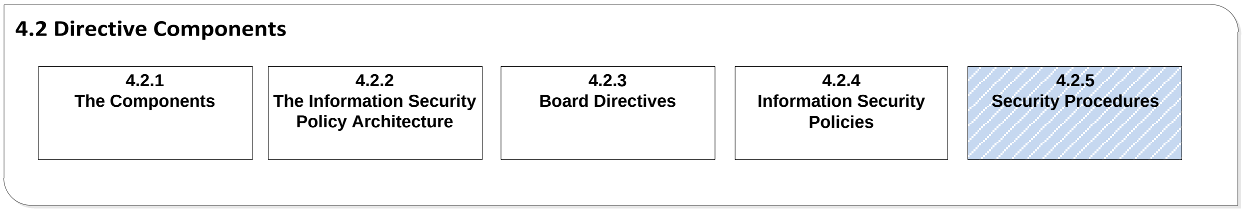
In contrast, an issue-specific policy will usually address specific technologies and applications in more detail; for example (S. Von Solms & Von Solms, 2008, p. 83):

- malicious software control
- acceptable internet usage
- acceptable email usage
- logical access control
- disaster recovery (backup)
- remote access control
- third-party access control

Thus, as an organisation makes use of various technologies and processes to support routine operations, it must instruct employees on the proper use of these technologies and processes (Whitman & Mattord, 2012, p. 181). These instructions are typically detailed in the above-mentioned policies where each gives specific information on a particular issue (S. Von Solms & Von Solms, 2008, p. 83). Consequently, they are frequently assigned the name of issue-specific policy (R. Von Solms et al., 2011). Moreover, owing to the level of detail given in these policies it is not uncommon to find them being updated frequently (Whitman & Mattord, 2012, p. 181).

Secondary-level policies thus expand on an organisation's corporate information security policy and form a significant part of the information security policy architecture (Bacik, 2008, p. 49). It is important to note here that, in order to inform the information security policy architecture, the origins of these secondary-level policies must be clearly indicated so as to ensure that they can be traced back to specific high-level statements in the corporate information security policy (S. Von Solms & Von Solms, 2008, p. 83). As S. Von Solms and Von Solms (2008, pp. 74–75) state, all documents in an information security policy architecture should form a hierarchical structure. Note that this structure does not end with the establishment of these policies. On the contrary, secondary-level policies are usually expanded in such a way that they offer actionable information in the form of security procedures to business operations and administration (R. Von Solms et al., 2011).

4.2.5 Security Procedures


4.2 Directive Components
4.2.1 The Components
4.2.2 The Information Security Policy Architecture
4.2.3 Board Directives
4.2.4 Information Security Policies
4.2.5 Security Procedures

For business operations to be executed in accordance to the relevant information security policies, and therefore the specified vision and strategy for information security, actionable information should be provided to ensure safe and secure information practices (Coertze et al., 2011). Operational-level management usually detail such actionable information by drafting security procedures that expand on the secondary-level policies established by tactical-level management (R. Von Solms et al., 2011).

Security procedures, also known as working instructions (Bacik, 2008, pp. 54–57), are “plans, processes or operations that address the detail of how to perform a specific action in a secure fashion” (Grobler & Von Solms, 2004, p. 3). Grobler and Von Solms (2004) indicate that security procedures typically answer the questions of *where*, *when* and *how* information security will be implemented and complied with, while the corporate information security policy and company standards answer *who*, *what* and *why* questions. These authors continue by specifying that procedures are normally the lowest-level documents in the information security policy architecture, as they contain very detailed systematic instructions for implementing the statements contained in the corporate information security policy and the secondary-level policies. It is thus clear that these procedures give valuable support for the directive components mentioned earlier.

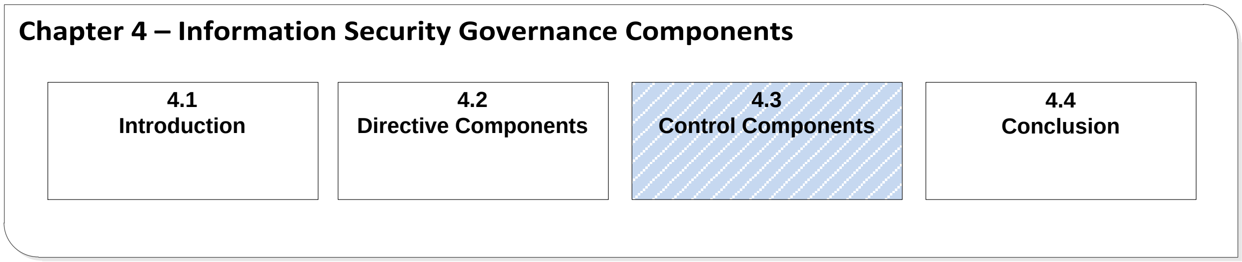
Further, it should be noted that there is not necessarily a simple relationship between secondary-level policies and security procedures, as some secondary-level policies may be supported by multiple procedures; similarly, a single procedure may be applicable to multiple secondary-level policies. Coertze et al. (2011) therefore state that the relationship between security procedures and secondary-level policies may be complex. This becomes clear when viewing the sample security procedures for the information systems acquisition, development and maintenance company standard found in Addendum C, p. 230.

During the drafting of security procedures, it is important to recognise the employee's or performer of the action's knowledge (Bacik, 2008, p. 54). Bacik (2008, p. 57) recommends that in the event that the employee is knowledgeable about an organisation's technologies and systems, operational-level management may opt to draft procedures that merely list the steps and actions required to perform a task in a secure fashion. By contrast, another option is to draft them graphically, where each step in the process could be represented using screenshots. Bacik (2008, pp. 54–55) notes that this second option is particularly suitable if an organisation is making use of contractual employees or outsourcing services. It can therefore be concluded that organisations can follow two different approaches when drafting security procedures.

To conclude, this section investigated the direct action of the direct–control action cycle established by S. Von Solms and Von Solms (2008, pp. 3–4). It introduced the components that facilitate this action, namely, board directives, information security policies and security procedures. Further, it was shown that these directive components usually form a hierarchical structure where each component adds support to the preceding component(s). This structure was termed the 'information security policy architecture' and was shown to be critical in the implementation of information security in an organisation.

Regrettably, the components that form this structure are only valuable if compliance, conformance and adherence to them can be assured and regulated (R. Von Solms & Von Solms, 2006a). Hence, the control action and the components that support it are essential if information security is to be successfully implemented and its governance confirmed. This action and its components will thus be investigated further in the following section.

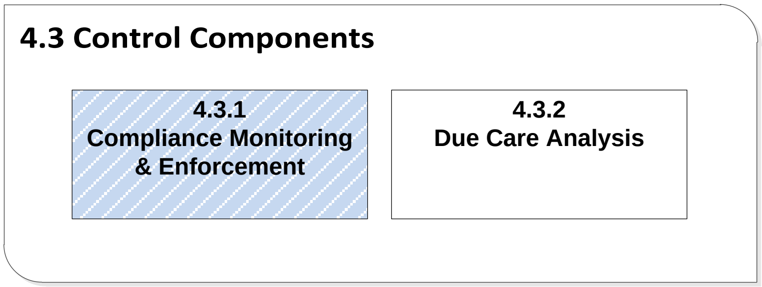
4.3 Control Components



The direct–control cycle for information security governance established by S. Von Solms and Von Solms (2008, pp. 3–4) clearly indicates that governance not only involves directing, but also necessitates control. Thus, for information security governance to be fully implemented, information security must be properly controlled to ensure that adherence to and compliance with the directive components, as outlined in the previous section, is truly being achieved (Brotby, 2009, pp. 146–147; S. Von Solms & Von Solms, 2008, p. 91). Hence, it is important to ensure that the management of information and IT risks is on an acceptable level.

Unfortunately, adherence to and compliance with the established directives of an organisation, including board directives and policies, are not always automatic as a result of human nature (West, 2008). Subsequently, components should be put in place to allow for monitoring and analysis to be performed in this regard. This section will thus discuss these components, namely, compliance monitoring and due care analysis, to gain a greater understanding of the control action exhibited by the direct–control action cycle.

4.3.1 Compliance Monitoring and Enforcement



Both ISO 27002 (2005) and CoBiT 5 (ISACA, 2012a) emphasise the importance of assuring conformance with an organisation’s policies, company standards and procedures. This is because human nature in general and employees in particular do not always conform to the wishes of executive management with regard to information security and secure information practices (West, 2008). Consequently, compliance enforcement and monitoring are vital for any information security governance implementation (S. Von Solms & Von Solms, 2008, p. 92).

R. Von Solms and Von Solms (2006a) indicate that compliance monitoring generally originates from business operations in which data will routinely be extracted from operational sources, such as log files and databases, or some other initiatives. These initiatives, which are used to overcome any limitations in operational sources, may include questionnaires, interviews or observations. This data is, in turn, used to produce operational-level compliance reports by comparing the activities performed to those actually specified in the organisation’s security procedures. Subsequently, these compliance reports are used by tactical-level management, which takes the extracted data and aggregates it to measure compliance with the requirements of the organisation’s secondary-level policies. Thereafter, strategic-level management typically receives from tactical-level management an aggregated or abstracted report of this comparison, which indicates compliance with the secondary-level policies. This report is further aggregated or abstracted to illustrate conformance and compliance with the corporate information security policy and the originating board directives.

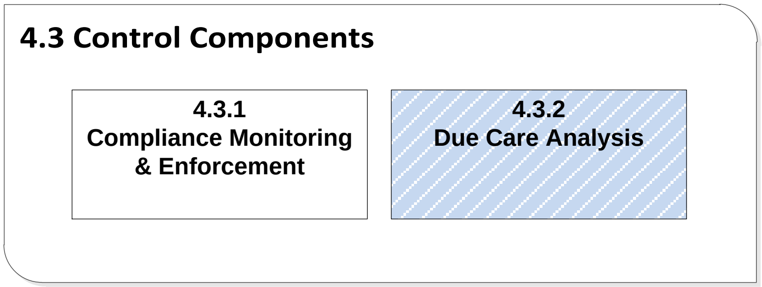
Regrettably, in order to perform monitoring of this nature, these components have to be measurable and, thus, there should be clear instructions for monitoring and enforcing compliance (S. Von Solms & Von Solms, 2008, p. 44).

S. Von Solms and Von Solms (2008, p. 93) recommend that compliance measuring processes should be implemented at regular intervals, if not real-time, in an organisation. However, in order to do this one needs to know which information and data to collect. Consequently, these authors indicate that measurability should be at the centre of all directive components produced during the direct action. It is no use having a statement, or clause, in a directive component if it cannot be measured. S. Von Solms and Von Solms (2008) therefore indicate that any statement(s) that cannot be measured for compliance should be excluded from these components, owing to the fact that these directive components only generate value if compliance can be enforced and measured by monitoring. Thus, these components will typically include statements that will indicate how compliance checking and measurability should be performed and evaluated. These statements are more formally known as ‘compliance clauses’ (S. Von Solms & Von Solms, 2008, p. 75). Compliance clauses play a vital role in the information security implementation process and will typically be tailored to an organisation and its directive components. However, owing to the tailoring and dynamic nature of the compliance clauses and, subsequently, their monitoring and enforcement, this remains one of the most difficult aspects to address and implement in an organisation (S. Von Solms & Von Solms, 2008, p. 93).

Once an organisation has established such clauses and put in place the means for monitoring compliance, it is essential that corrective action is taken in areas where the envisaged compliance is lacking (David, 2002). This will ensure that compliance is enforced and that the secure practices of an organisation will improve over time. Enforcement in this regard may take on many different forms (Herath & Rao, 2009). One form may be that additional directive components are introduced for the area(s) that are lacking; another may be that penalties are introduced for non-compliance (Bacik, 2008, p. 138). Irrespective of the form enforcement takes, organisations must ensure that such enforcement takes place, otherwise the establishment and monitoring of directive components may fail to provide any substantial benefits as security breaches may continue to occur.

From the discussion it is evident that compliance monitoring on all operating levels of an organisation is vital to the successful implementation and governance of information security. It is, however, important to note that an organisation's executive management is not exempt from such monitoring and enforcement and therefore it too may face routine evaluation and analysis of its information security governance duties.

4.3.2 Due Care Analysis



Compliance monitoring and enforcement will typical involve management from the operational to the tactical level (Coertze et al., 2011), but usually does not include executive management. Consequently, executive management may come to believe that it is exempt from monitoring and evaluation. This is not the case, however, as executive management should be monitored and evaluated in terms of the due care and due diligence they provide for information security (R. Von Solms & Von Solms, 2006b), which is a predefined duty of information security governance (Brotby, 2009, p. 86).

R. Von Solms and Von Solms (2006b) suggest in this regard that the monitoring and evaluation should take the form of a due care analysis exercise. They state further that a due care analysis exercise typically consists of a series of questions posed to executive management. These questions focus on determining whether, with the implementation of information security, due care or due diligence is being met (R. Von Solms & Von Solms, 2006b). Hence, due care and due diligence comprise a central theme of such an exercise.

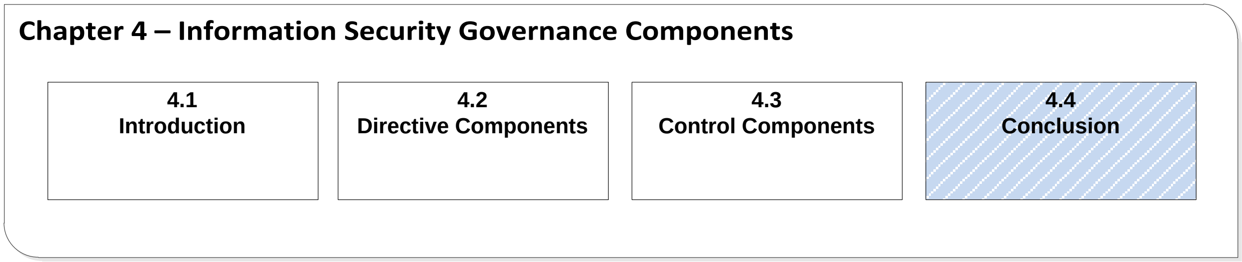
Whitman and Mattord (2012, p. 585) define due care in this regard as “the actions that demonstrate that an organisation makes sure that every employee knows what is acceptable or not acceptable behaviour, and knows the consequences of illegal or unethical actions”. Similarly, they define due diligence as “the actions that demonstrate that an organisation is diligent in ensuring that the implemented standards continue to provide the required level of protection”. Failure to provide either due diligence or care, may result in an organisation facing legal liability as a result of the fact that it may be viewed as negligent (S. Von Solms & Von Solms, 2008, p. 122).

Negligence may be defined as “the failure to exercise that degree of care that, in the circumstances, the law requires for the protection of other persons or those interests of other persons that may be injuriously affected by the want of such care” (Dictionary.com, 2012). In order for organisations to avoid claims of negligence, it is crucial that due care analysis be performed and corrective actions taken if necessary.

An example of a due care analysis exercise may be found in the journal article titled “Information security governance: Due care” (R. Von Solms & Von Solms, 2006b). In this article a due care analysis exercise is presented consisting of a series of questions, which are posed to executive management in order to examine the level of due care and diligence undertaken. Based on the response(s) to these questions, the exercise offers a clear indication as to whether due care and diligence is being taken with regard to information security. Once this indication is obtained, it is essential that corrective action(s) be taken by the parties if any element of due care or diligence is lacking. This is crucial if an organisation wishes to avoid legal liability and prosecution in a court of law (Gerber & Von Solms, 2008).

To conclude, this section investigated the control action of the direct–control action cycle established by S. Von Solms and Von Solms (2008, pp. 3–4). It introduced the components that facilitate this action, namely, compliance monitoring and due care analysis. Further, it was shown that directive components only have value if compliance, conformance and adherence to them can be ensured and regulated. Hence, the control action and supportive components, in conjunction to those of the direct action, were shown to be essential for information security implementation and governance.

4.4 Conclusion

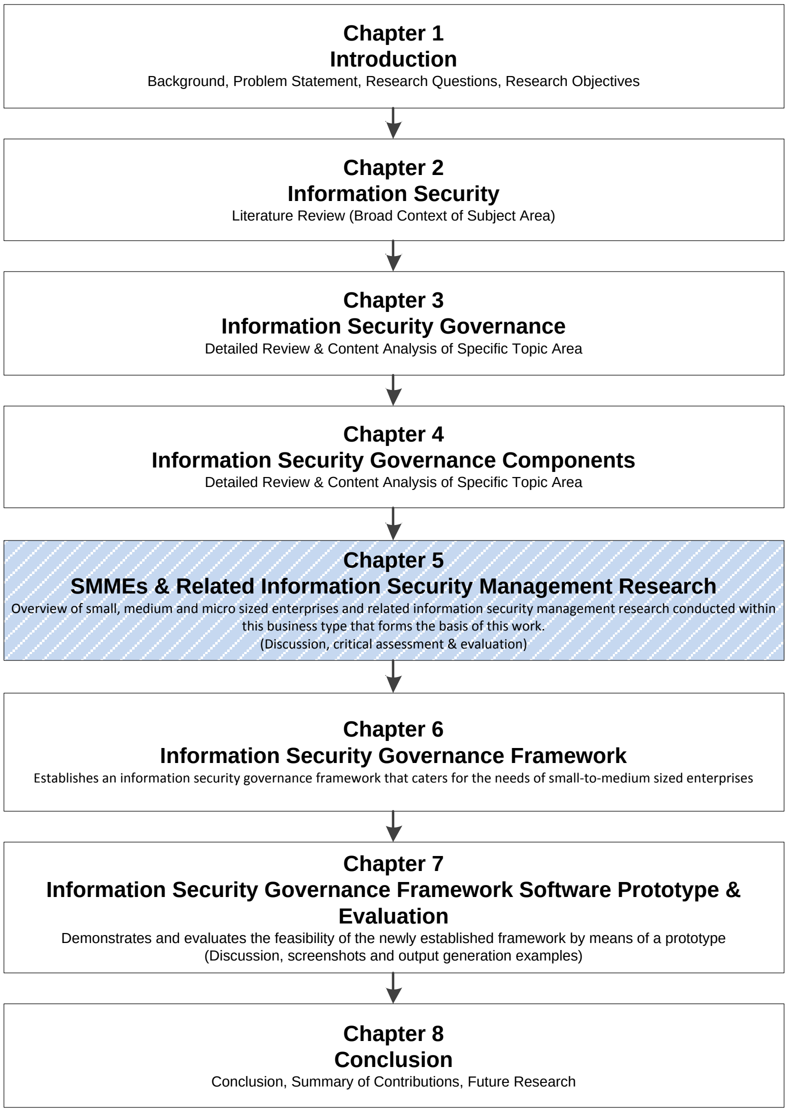


Information security governance requires several components to be implemented in an organisation in order to allow executive management to both direct and control information security (S. Von Solms & Von Solms, 2008). Without these components being addressed and implemented, information security governance is almost sure to fail or will face significant difficulties (Bacik, 2008, p. 18). In view of this, and the fact that this work aims to formulate an information security governance framework, this chapter introduced and discussed these components in order to offer evidence as to why they should exist, their purpose and how they may assist in the information security governance process.

Rees (2010), Tawileh et al. (2007) and Yildrim et al. (2010) all agree however that SMMEs are struggling to implement the components that have been discussed here and are subsequently experiencing difficulties implementing information security governance. This is especially concerning as these enterprises form a significant part of any country's economy (Raynard & Forstater, 2002, p. 2) and are starting to rely more heavily on information and information technologies (Gupta & Hammond, 2005). Consequently, this work aims to contribute to resolving this problem. However, in order to do so these enterprises and their problems with information security governance first have to be investigated. This forms the primary focus of the following chapter which explores research conducted in this area.

Chapter 5: SMMEs and Related Information Security Management Research

This chapter aims to investigate SMMEs by highlighting their importance, their unique business characteristics, their dependence on IT and their requirement for information security. Further, it aims to present research on information security management that has previously been conducted in this field.



Chapter 1
Introduction
Background, Problem Statement, Research Questions, Research Objectives

Chapter 2
Information Security
Literature Review (Broad Context of Subject Area)

Chapter 3
Information Security Governance
Detailed Review & Content Analysis of Specific Topic Area

Chapter 4
Information Security Governance Components
Detailed Review & Content Analysis of Specific Topic Area

Chapter 5
SMMEs & Related Information Security Management Research
Overview of small, medium and micro sized enterprises and related information security management research conducted within this business type that forms the basis of this work.
(Discussion, critical assessment & evaluation)

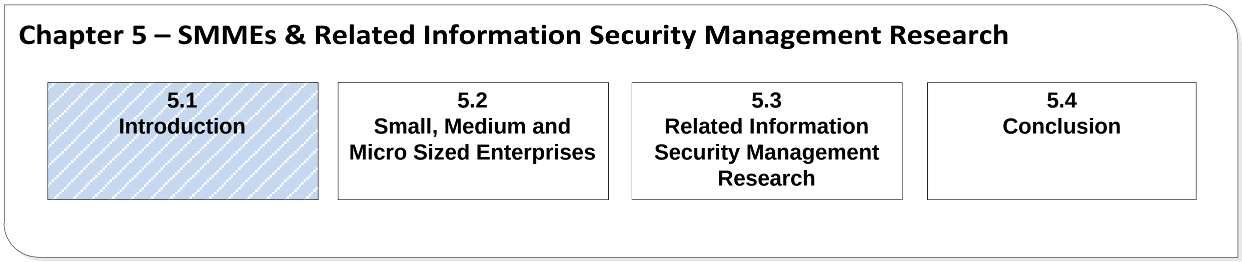
Chapter 6
Information Security Governance Framework
Establishes an information security governance framework that caters for the needs of small-to-medium sized enterprises

Chapter 7
Information Security Governance Framework Software Prototype & Evaluation
Demonstrates and evaluates the feasibility of the newly established framework by means of a prototype
(Discussion, screenshots and output generation examples)

Chapter 8
Conclusion
Conclusion, Summary of Contributions, Future Research

“*Protect the business – never think it is too small to be a target for malicious attack from hackers, malware or a disgruntled employee*” (Rees, 2010, p. 19)

5.1 Introduction



Chapter 5 – SMMEs & Related Information Security Management Research
5.1 Introduction
5.2 Small, Medium and Micro Sized Enterprises
5.3 Related Information Security Management Research
5.4 Conclusion

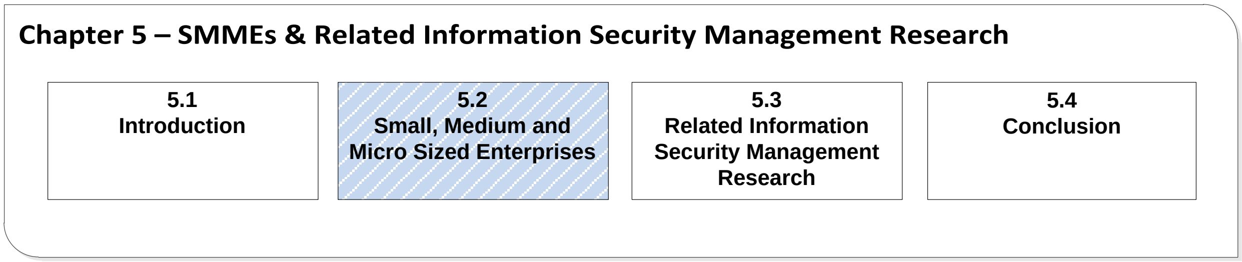
Small, medium and micro-sized enterprises (SMMEs) form a major part of economies around the world (Sánchez, Ruiz, Fernández-Medina, & Piattini, 2010). Countries and economies alike have come to depend on this category of business to make unique economic contributions, including innovation and flexibility (Koornhof, 2009, p. 28; Le Roux, 2010, p. iv). Moreover, they provide essential employment for large numbers of citizens who cannot find employment in larger organisations (Baskerville, Dhillon, & Stahl, 2011).

In many countries the use of information and information technologies is being introduced to these enterprises in order to afford them opportunities for essential growth and competitiveness (Bhattacharya, 2008, pp. 75–76; Stanley, 2010). Although such benefits can certainly be obtained, they cannot be achieved without considering information security, as this not only contributes to the wellbeing of large businesses, but also to this smaller category of businesses (S. Von Solms & Von Solms, 2008). Thus, as dependence on information and its supporting technologies increases, so should an awareness of the importance of information protection (ISO/IEC 27002, 2005). It is disappointing to note that the literature suggests that this protection remains a significant challenge for these enterprises (Yildirim et al., 2010). This is especially true of information security governance, where it is often found that such enterprises lack the resources and/or expertise to implement it properly (Le Roux, 2010, p. 9).

Fortunately, research has been conducted with the aim of addressing this problem; one such research study has led to the formulation of an information security management framework (Vermeulen & Von Solms, 2002). However, the vast evolution in IT dependency, cloud computing and 'bring your own device' (BOYD) that has been witnessed globally, as well as the requirement for proper information security governance, have resulted in some shortcomings being identified in this framework (Coertze et al., 2011). Consequently, if the current information security issues that these enterprises are facing are to be adequately addressed, the shortcomings identified in the framework must be investigated and subsequently resolved. Hence, the establishment of a revised framework forms the primary objective of this research.

These issues will be discussed in detail in this chapter as follows: Firstly, a discussion on small, medium and micro-sized enterprises (SMMEs) is provided. Specific mention will be made of the importance and unique business characteristics of these enterprises, as well as the current information security issues that they are facing. Secondly, information security management research that has previously been conducted to assist in resolving some of these issues will be introduced and key concepts explained. Finally, a discussion of the shortcomings of the related research will conclude the chapter in order to argue for the need of an information security governance framework.

5.2 SMMEs


Chapter 5 – SMMEs & Related Information Security Management Research
5.1 Introduction
5.2 Small, Medium and Micro Sized Enterprises
5.3 Related Information Security Management Research
5.4 Conclusion

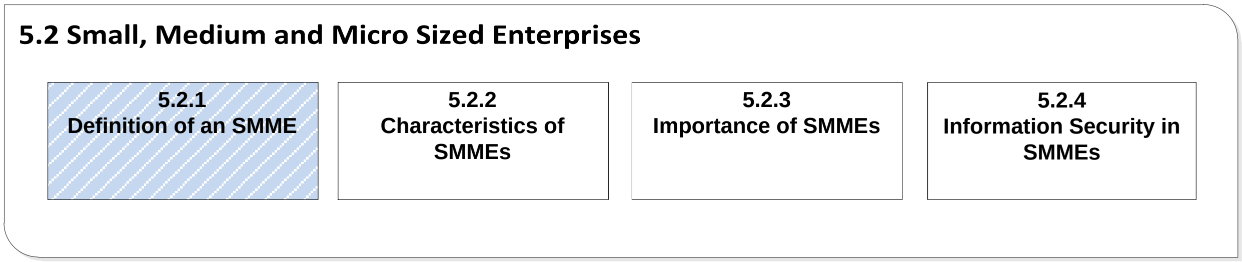
Although the term 'SMME' is used widely in the literature and throughout the world, there is no universal definition of the concept (Andreassen, 2011, p. 16; Smit & Watkins, 2012). This may be as a result of the fact that there are many distinctive business characteristics that differentiate these businesses from their larger counterparts. Some of these characteristics include their size, location, ownership structure, financial (turnover level) performance, maturity and management style (Devos et al., 2012).

Irrespective of the definition used, it is well known that these enterprises play a significant role in any country's economy (Chiware & Dick, 2008). This is because they offer substantial employment opportunities and often receive investment from foreign investors owing to their innovative and flexible nature (Raynard & Forstater, 2002, p. 3).

Unfortunately, information security remains a challenge for these enterprises, which is all too often seen as daunting or simply impossible to address (Gupta & Hammond, 2005; Upfold & Sewry, 2005; Yildirim et al., 2010). As a result, the success of these enterprises is being placed at severe risk, as their dependence on information and in particular IT continues to grow (Stanley, 2010; Wall, 2005).

In order to assist these organisations with their information security challenges and afford valuable insight into the framework to be established by this research, it is essential to obtain a clear understanding of the specifics of this business category. This will be accomplished in the following section, which will firstly define SMMEs, secondly, highlight their importance and their unique business characteristics and, finally, investigate their current information security challenges.

5.2.1 Definition of an SMME



5.2 Small, Medium and Micro Sized Enterprises

5.2.1 Definition of an SMME

5.2.2 Characteristics of SMMEs

5.2.3 Importance of SMMEs

5.2.4 Information Security in SMMEs

What is a small, medium and micro-sized enterprise? Initially this might seem to be a fairly straightforward question; however, as one delves deeper into the topic, it becomes clear that defining an SMME is no simple matter.

Small, medium and micro-sized enterprises, typically abbreviated as SMME, are found in countries throughout the world (Beachboard, Cole, Mellor, Hernandez, & Aytes, 2008). They constitute a significant portion of any country's economy and are important for the employment opportunities they provide. It is thus clear that these enterprises are crucial for economic growth and development. Although much research and development has taken place in this business type, no universal definition exists (Boubala, 2010, p. 26).

It is argued that the lack of a common definition may perhaps be a result of the sheer number of SMMEs that operate throughout the world (Koornhof, 2009, p. 17). Added to this is the fact that many other characteristics beyond size differentiate these businesses from their larger counterparts (Devos et al., 2012). Moreover, the geographical location of such a business can also have a significant impact on the definitions used, as they differ from one country to the next (Smit & Watkins, 2012).

Most countries have their own definitions or classifications for SMMEs for legal reasons or for issuing loans and grants (Koornhof, 2009, p. 12). Some of these classifications may refer to qualitative measures, while others may use quantitative measures or a combination of both (Boubala, 2010, p. 27). These measures include the number of employees, monetary value of capital assets, turnover levels, legal status, production methods and operating industries (Andreassen, 2011, p. 16; Koornhof, 2009, p. 12).

Although it is evident that a common definition for SMMEs does not exist, there are a select few that are often referred to in the literature. Two definitions in this regard, include the definition of the South African National Small Business Act (1996; 2003; 2004) and the European Union (EU Recommendation 361, 2003). These two definitions are of specific interest to this work, as they encompass not only SMMEs operating in South Africa, but also in the rest of the world.

The South African National Small Business Act (1996; 2003; 2004) defines SMMEs in terms of the number of employees, turnover levels and gross asset value. According to this definition, all businesses operating with fewer than 200 employees, less than R64 million turnover per annum and less than R23 million in gross asset value fall into this business type.

Similarly, the definition originating from the European Union (EU Recommendation 361, 2003) indicates that all businesses operating with fewer than 250 employees, less than €50 million turnover per annum and less than €43 million in gross asset value may be considered an SMME.

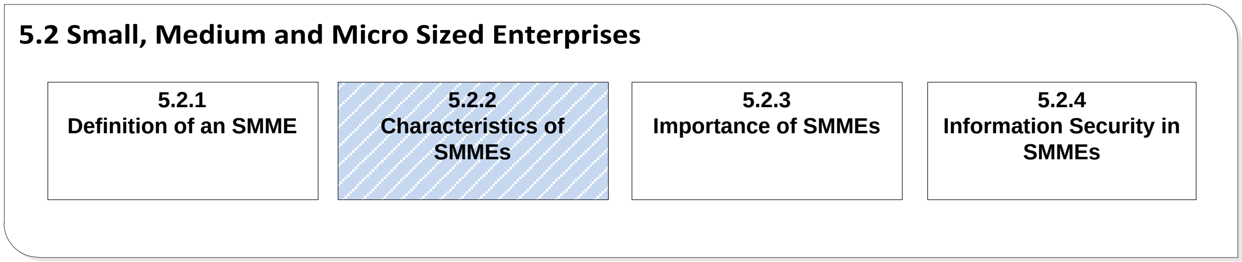
These two definitions are detailed further in Table 5.1.

Table 5.1 – Definition of SMMEs in different regions (Andreassen, 2011, p. 17)

	South Africa			European Union		
Category	**Employees**	**Turnover in R (million)**	**Gross asset value in R (million)**	**Employees**	**Turnover in € (million)**	**Gross asset value in € (million)**
Micro	Up to 5	0-0.2	0-0.1	Up to 10	Up to 2	Up to 2
Very Small	Up to 20	Up to 6	Up to 2	N/A	N/A	N/A
Small	Up to 50	Up to 32	Up to 6	Up to 50	Up to 10	Up to 10
Medium	Up to 200	5-64	5-23	Up to 250	Up to 50	Up to 43

There is, thus, a clear correlation between these two definitions as both use similar measures for classification purposes. However, irrespective of the definition used, it is clear that these enterprises exhibit unique business characteristics not found in larger organisations (Devos et al., 2012). These may include limited staff, turnover and gross asset value all resulting in restricted availability of resources and expertise for business operations, and especially information security governance implementation (Goucher, 2011). However, before the importance and security issues of these enterprises can be considered, it is vital to understand the unique business characteristics that they exhibit and differentiate them from larger organisations.

5.2.2 Characteristics of SMMEs


5.2 Small, Medium and Micro Sized Enterprises
5.2.1 Definition of an SMME
5.2.2 Characteristics of SMMEs
5.2.3 Importance of SMMEs
5.2.4 Information Security in SMMEs

Having defined SMMEs in the previous subsection, it now becomes possible to investigate their unique characteristics and to differentiate them from larger organisations. SMMEs operate in the same environment as their larger contemporaries, but exhibit very distinct characteristics and traits (Smit & Watkins, 2012). Some might believe all organisations to be the same, but this is unfortunately not true. Whereas large organisations were traditionally believed to have near total and unrestricted access to resources, SMMEs often do not have this luxury (Wong, 2005). Moreover, organisational structure, size and financing channels may also differ (Xiaoping & Jing, 2008).

SMMEs are to be found in many different forms (Levy, 2009, p. 6) and are usually born out of entrepreneurial passion focused on addressing a single core business concept (Upfold & Sewry, 2005). As a result, they rarely concern themselves with peripheral activities that are not core to their concept (Beachboard et al., 2008). It is this dedicated focus which often allows them to be incredibly flexible and innovative (Beachboard et al., 2008). Unfortunately this comes at a price, as business decisions in these enterprises must often be made without any prior preparation (Barlette & Fomin, 2008). Consequently, these enterprises are frequently stated as having very high failure rates (Sánchez et al., 2010).

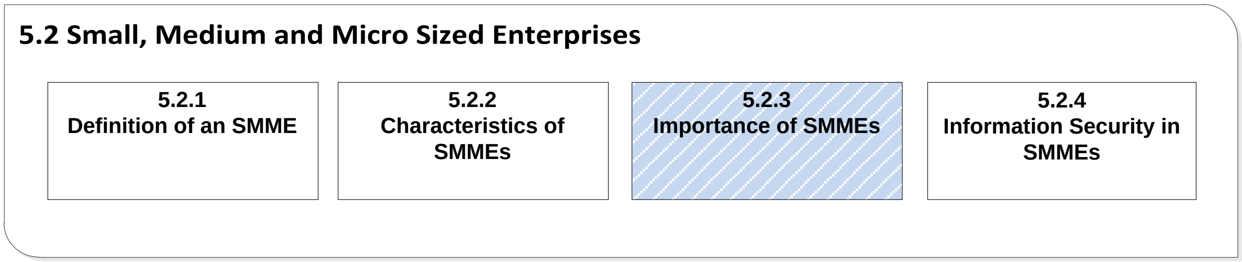
SMMEs face many daily pressures, which certainly contribute to the high rates of failure (Smit & Watkins, 2012). Some of these pressures may include a lack of staff, processes, technology and even specialised knowledge (Krishna, 2010, p. 2). Hence, the term 'resource poverty' is often attributed to these enterprises, signifying that crucial resources are not always easily attainable by them (Koornhof, 2009, pp. 82–83). Added to this, it is often found that these enterprises lack the management skills necessary for adequate corporate governance to take place (Smit & Watkins, 2012). Together this combines to create a situation in which these enterprises may be placed under enormous stress and may become extremely vulnerable to closing down (Le Roux, 2010, p. 9).

Within a large organisation, ownership and management is normally distanced, whereas in SMMEs the owner(s) may fulfil both roles simultaneously (Beaver & Prince, 2004). In these enterprises acquisitions and decision making often rest purely on the shoulders of the owner (Levy, 2009, p. 7), with the result that the owner is frequently viewed as holding the most influence in these enterprises (Huang, Zmud, & Price, 2009). This is especially true of very small micro enterprises, where a management structure may be vastly different, or in some cases be non-existent, differentiating them from small and medium enterprises. Unfortunately, this is not ideal as secondary decisions and tasks, necessary for business operations, are often placed on the backburner as the owner might not have adequate time or the necessary skills to deal with them (Gupta & Hammond, 2005). Consequently, the owner's focus is often exclusively drawn to the core business function essential for continued success (Beachboard et al., 2008). This characteristic is noted; however the remainder of this work will focus more specifically on small and medium enterprises when referring to SMMEs, as their management structure more closely supports and recommends the components of the framework and supportive software prototype that forms the solution of this work. Hereby the usage of the framework and supportive software prototype by micro enterprises is not voided or diminished, but it may be necessary for such an enterprise to selectively choose components from the solution that's more applicable to them.

These and other constraints placed on these enterprises often result in them having a heavy reliance on outsourcing and external consultants (Xiaoping & Jing, 2008). Although this approach may seem appropriate and beneficial in theory, these enterprises' financial standing often makes it impossible to afford (Upfold & Sewry, 2005). Consequently, much research and development has been conducted to assist these enterprises in addressing their constraints using other avenues of operation. One of the areas that has seen much focus in this regard is that of information and IT (Coertze et al., 2011; Vermeulen & Von Solms, 2002; Wall, 2005).

Owing to the availability of the internet and the affordability of the modern computer unit, governments around the world are rapidly introducing and recommending IT for adoption by SMMEs (Barlette & Fomin, 2008). Wall (2005) indicates that this has especially taken place in Europe and various Asian countries like Japan, China and India. Consequently, these enterprises are expanding their business operations by making use of larger networks, enabling mobile workforces and establishing websites (Stanley, 2010; Sumner, 2009). Added to this these enterprises are now also leveraging e-commerce, allowing them to target markets that were previously reserved for larger organisations, making use of cloud computing for storage and allowing staff to bring their own devices to the work place to reduce operating costs (Bhattacharya, 2008, p. 64). Altogether this is allowing these enterprises to gain significant benefits, including reduction in poverty and increases in productivity (Burns et al., 2006). These benefits in turn are raising the importance of SMMEs within the global and local economies around the world.

5.2.3 Importance of SMMEs


5.2 Small, Medium and Micro Sized Enterprises
5.2.1 Definition of an SMME
5.2.2 Characteristics of SMMEs
5.2.3 Importance of SMMEs
5.2.4 Information Security in SMMEs

Throughout the previous subsections mention has been made of the importance of SMMEs to the economic prosperity of a country. SMMEs make a significant contribution to any country's economy by securing economic, social and environmental sustainable development (Devos et al., 2012; Raynard & Forstater, 2002, p. 2).

SMMEs can be found operating throughout the world and help countries and their larger counterparts to achieve their goals (Beachboard et al., 2008). As Raynard and Forstater

(2002, p. 2) indicate, nearly 90% of businesses worldwide can be classified as small, medium or micro-sized. Smit and Watkins (2012) suggest that in First World countries, such as America and the United Kingdom, they can account for as much as one-third of employment and a slightly lower percentage of output. They also mention that for Third World countries these figures may even be higher, as they dominate markets in these countries and add valuable employment opportunities which otherwise may not have existed. These enterprises therefore make up an important part of the business fabric and employment opportunities of any country (Sánchez et al., 2010).

SMMEs are said to account for over 50% of the total employment opportunities in countries around the world (Andreassen, 2011, p. 18). They thus offer significant job creation opportunities, which in turn may aid in economic growth and the alleviation of poverty (Chiware & Dick, 2008). This is important not only for developed First World countries, but especially for developing countries around the world (Raynard & Forstater, 2002, p. 2).

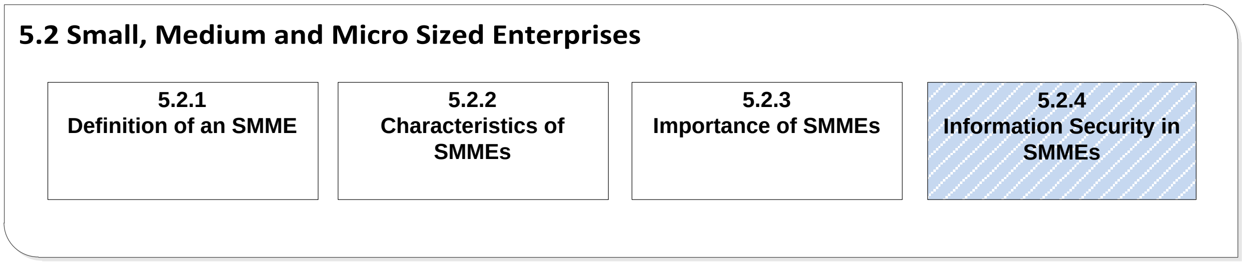
Statistics indicate that developing countries are highly dependent on SMMEs for successful operation and growth (Andreassen, 2011, pp. 18–19). Smit and Watkins (2012) state that this is particularly true of African nations, such as Togo, Uganda, Nigeria, as well as others. They suggest that this may be because such enterprises are labour intensive, generate significant income and thus reduce poverty (a major concern for these countries). Further, in developing countries these enterprises typically complement larger organisations by offering supportive services and products necessary for business operations (Rogerson, 2004). In turn, this allows larger organisations in these countries to remain competitive, which promotes additional revenue flowing into the local economy. It is thus clear that these enterprises are highly beneficial to the overall success and operation of a country's economy (Goucher, 2011; Raynard & Forstater, 2002, pp. 2–3).

In summary, SMMEs are considered important for the following reasons (Megginson, Byrd, & Megginson, 2006, p. 9):

- "They offer more job opportunities than other sized organisations;
- They keep larger organisations competitive;
- They encourage flexibility and innovation;
- They offer opportunities for aspiring entrepreneurs who are unemployed, underemployed or retrenched;
- They provide employees with limited or no skills and training comprehensive learning experiences; and
- They operate more closely with the community and their customers."

Although the importance of SMMEs has been established and their unique business characteristics defined, it now becomes essential that the current information security challenges of these enterprises are identified and understood as this form the primary focus of this work.

5.2.4 Information Security in SMMEs


5.2 Small, Medium and Micro Sized Enterprises
5.2.1 Definition of an SMME
5.2.2 Characteristics of SMMEs
5.2.3 Importance of SMMEs
5.2.4 Information Security in SMMEs

SMMEs are ever important within the global and local economies of the world and are starting to utilize IT, cloud and various other technologies to greater extends. Although the benefits from utilization of these technologies cannot be ignored, it should be kept in mind that the security required and the risks involved also have to be addressed (ISO/IEC 27002, 2005, p. viii).

Kankanhalli, Teo, Tan and Wei (2003) argue that as organisations become increasingly dependent on information and IT for strategic advantage and operation, the issue of information security also becomes increasingly important. Thus, as SMMEs are increasingly using information and IT, particularly for conducting e-commerce, they too should view information security as critical to the business. (S. Von Solms & Von Solms, 2008, p. 139)

Unfortunately, SMMEs often consider larger organisations to be more at risk from security incidents than themselves (Rees, 2010); this is not the case as statistics indicate that these enterprises are actually more at risk because they may face more security incidents than their larger counterparts (McAfee, 2009). This results in the so-called 'security paradox' where these enterprises may believe information security not to be a major concern, while in truth it should be viewed as the exact opposite (Stanley, 2010).

SMMEs face serious security challenges (Kimwele, Mwangi, & Kimani, 2011). Research indicates that, within a year (Koornhof, 2009, p. 73):

- 41% of these enterprises may experience a loss of network availability as result of a security incident
- 41% may fall victim to computer viruses, worm or Trojan horse attacks
- 19% may experience security breaches which could result in more than 24 hours of downtime.

These statistics are particularly alarming as a single breach may put an SMMEs totally out of business (McAfee, 2009), since these businesses cannot function for more than a few hours without information and IT being available (Horn, n.d.). Consequently, if information security is not adequately addressed, it could yield catastrophic results for these enterprises and the local economy (Kimwele et al., 2011). This is particularly true as such security incidents cost affected enterprises around the world trillions every year (McAfee, 2009). This is an alarming statistic for developing countries, since these costs could contribute to the downfall of a local economy.

Unfortunately, SMMEs generally do not perceive information security as being critical (Dojkovski, Lichtenstein, & Matthew, 2007). This may be because the owners are often unaware of its importance or may not have the necessary resources to facilitate its implementation (Gupta & Hammond, 2005; Krishna, 2010, pp. 2, 7). Further, if the owner does not perceive information security to be critical, then the rest of the organisation often follows. This results in a situation where information security regularly receives little attention in these enterprises (Beranek, 2011).

Thus, information security habitually receives low prioritisation by these enterprises, as other business aspects are often believed to be more critical since limited time and restricted funds are available (Gupta & Hammond, 2005). Therefore, it should come as no surprise that many of these enterprises simply do not implement information security, as it requires time, money and effort which they are unwilling to invest (Barlette & Fomin, 2008). However, as Rees (2010) indicates: the business must be protected at all costs, especially if it wants to experience successful growth and continued prosperity.

This protection, in the form of information security and its governance, involves several components. These components include board directives, information security policies and compliance monitoring to name but a few (S. Von Solms & Von Solms, 2008, p. 74). Unfortunately, these enterprises are experiencing great difficulty in implementing and maintaining some of these components (Coertze et al., 2011; Gupta & Hammond, 2005; Upfold & Sewry, 2005).

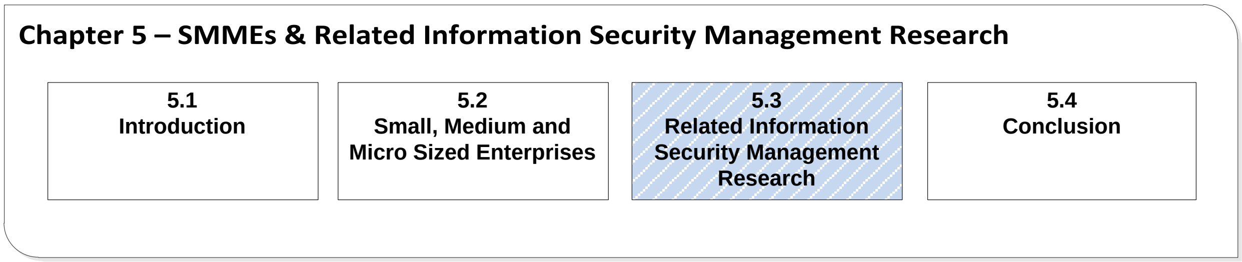
Research conducted by Upfold and Sewry (2005) in the Eastern Cape found that SMMEs typically did not have adequate information security and governance. The research found that although many frameworks exist for information security governance, they do not take into account the constraints placed on SMMEs. Similar research conducted by Yildirim et al. (2010) agrees with this finding, showing that up to 58% of respondents found their information security governance and contributing components to be ineffective.

This is further supported by Gupta and Hammond (2005), who found that many SMMEs were so preoccupied with day-to-day operations that they neglected to address information security and its governance adequately. The research also found that information security, in many cases, was only seen as necessary once the business had faced a serious information security breach. Consequently, it was found that only 48% of their respondents had some form of written information security policy. This finding of inadequate policy drafting and potential lack of compliance monitoring is also supported by Upfold and Sewry (2005), Burns, Davies and Davies (2006) and Yildirim et al. (2010).

It can therefore be concluded that these enterprises often struggle to implement and maintain information security governance components, such as information security policies (Upfold & Sewry, 2005). This is perhaps a consequence of the lack of in-house information security knowledge or expertise which is often experienced within these businesses (Koornhof, 2009, p. 83; Yildirim et al., 2010). This may be as a result of the many problems they face in recruiting qualified or experienced personnel, since their unique characteristics often do not appeal to job applicants (Barlette & Fomin, 2008).

From this discussion, it should be clear that information security, and the governance thereof, remains a serious challenge for these enterprises (Sumner, 2009). Fortunately, research has been conducted in order to aid them in this regard (Hoppe et al., 2002; Vermeulen & Von Solms, 2002).

5.3 Related Information Security Management Research


Chapter 5 – SMMEs & Related Information Security Management Research
5.1 Introduction
5.2 Small, Medium and Micro Sized Enterprises
5.3 Related Information Security Management Research
5.4 Conclusion

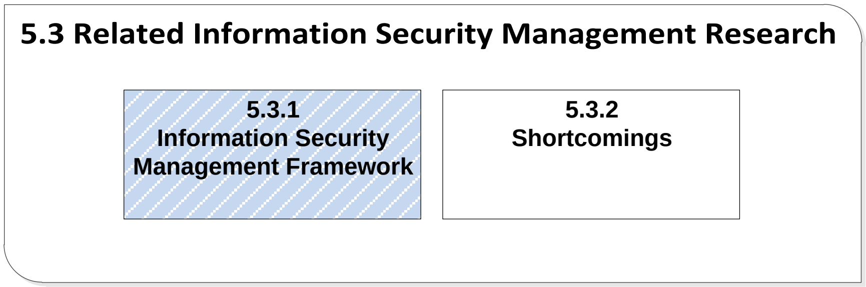
SMMEs make up a large part of the economy of countries around the world (Sánchez et al., 2010) and in all these countries they are facing many challenges (Koornhof, 2009, p. 11), of which information security is a major concern (Gupta & Hammond, 2005). Many of these enterprises believe information security to be a solely technical intervention (Kimwele et al., 2011) and, as a result, many have inadequate information security implementation and measures (Bougaardt & Kyobe, 2011). A major contributing factor with regard to this finding is that many of these enterprises are in a financial position that does not allow them to hire specialised security professionals and consultants to implement and monitor security measures. Therefore, these enterprises often lack the in-house knowledge required to address information security and its governance adequately (Coertze et al., 2011).

In order to aid these enterprises in resolving this situation, an information security management framework has been created as a result of previous research (Vermeulen & Von Solms, 2002). This was subsequently implemented and used as the foundation to create a software application prototype (Hoppe et al., 2002). Both the framework and the prototype, as the name suggests, focus specifically on assisting organisations to manage information security properly.

As this work aims to develop a comprehensive information security governance framework, the previously mentioned research is of specific interest since management and governance are closely correlated. Further, the working prototype of the previous research also forms the basis for the prototype that has resulted from this study, since additional components will be added to the original to facilitate the new concepts in the forthcoming framework.

There is thus a close relation between the works of Vermeulen and Von Solms, the Information Security Management Toolbox developed by Hoppe et al. and this work. Consequently, the following section will introduce the reader to the underlying concepts and shortcomings of the information security management framework and supportive software prototype. This, in turn, will help to identify the reasons why an information security governance framework should be established to address the inadequacies identified in the existing framework.

5.3.1 Information Security Management Framework



The framework shown in Figure 5.1 was previously developed for use by organisations to manage information security properly (Vermeulen & Von Solms, 2002). The framework consists of a series of elements, each of which was perceived as contributing to the successful implementation of information security management. This was formulated in terms of various phases. These phases include the preparation, implementation and maintenance of a management system.

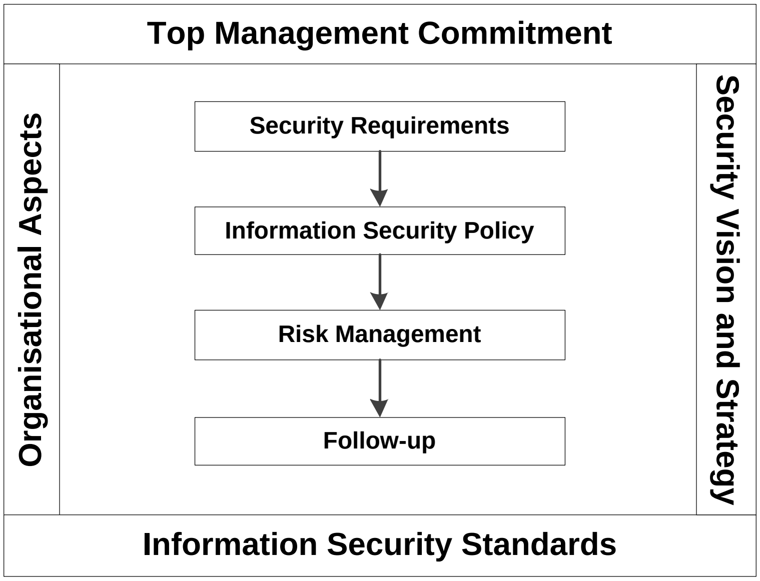

Top Management Commitment
Organisational Aspects
Security Requirements
Information Security Policy
Risk Management
Follow-up
Security Vision and Strategy
Information Security Standards

Figure 5.1 – Information security management framework (Vermeulen & Von Solms, 2002)

The framework suggests that the preparation phase, which can be seen on the outer edges of Figure 5.1, includes initial elements such as top management commitment in combination with the investigation of the information security standards to be used in the organisation. The framework further consists of introductory elements such as addressing organisational aspects, which is vital to ensure that roles and responsibilities are established for information security, as well as the establishment of a security vision and strategy.

Thus, during the preparation phase it is vital that top management commitment is sought, as this is the level that is ultimately responsible for information security in an organisation, as well as having the authority to ensure that subordinates will follow its vision and strategy. After such commitment is received, information security standards can be investigated to offer supportive information by establishing an approach to implement an information security management system in the organisation. In this regard, it is also vital that an organisational structure should be established so as to ensure that the staffing needs are met in order to reach the required information security levels. After these preparatory elements have been addressed, the implementation phase of an information security management system can commence.

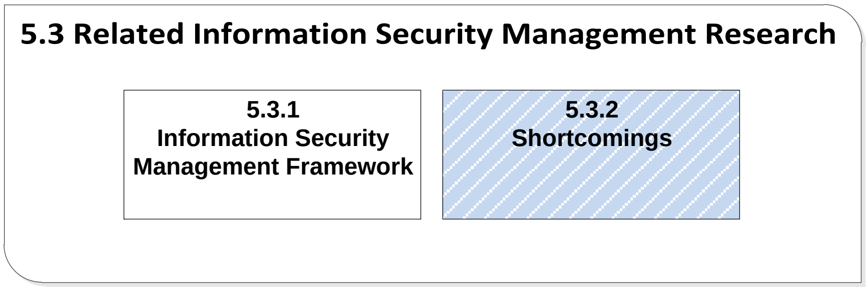
The implementation phase, as indicated in the core of Figure 5.1, consists of elements that include the establishment of security requirements, the drafting of information security policies and risk management. Vermeulen and Von Solms (2002) indicate that these elements can be viewed as a sequential process; thus each element should be addressed systematically. Consequently, the process commences with the formalisation of security requirements, typically by means of a risk analysis. Once established, these security requirements facilitate the drafting of so-called information security policies. These policies then form the foundation on which information security management can be based in an organisation. Subsequently, the drafting of these policies enable risk management to be performed, which entails the selection and implementation of various safeguards and procedures based on the recognised security requirements.

It is of importance to note that Vermeulen and Von Solms (2002) indicate that information security management is an on-going process and thus not a once-off activity. As a result, they suggest that a maintenance stage is essential for information security management to be successfully implemented. It is essential to note that they did not explicitly indicate this in the framework, although they did add a *follow-up* element, which may be viewed as being representative of this.

To conclude, this information security management framework provides a variety of elements that are essential for both the introduction and the on-going maintenance of information security management in an organisation. This framework in turn facilitated the development of a methodology for the widespread implementation of information security management in most organisations, which could comply with modern information security management requirements (Vermeulen & Von Solms, 2002). Unfortunately, the authors found that organisations often do not have the expertise or resources to implement this framework or the methodology and, subsequently, a working software application prototype was developed to automate certain steps (Hoppe et al., 2002).

Although this related research has proven to be feasible and effective in the past (Vermeulen & Von Solms, 2002), the vast change in the dependency on IT witnessed globally, as well as the requirements for proper information security governance, have resulted in some inadequacies coming to light. These will be discussed in more detail in the following subsection.

5.3.2 Shortcomings


5.3 Related Information Security Management Research
5.3.1 Information Security Management Framework
5.3.2 Shortcomings

The dependency on information and IT is increasing rapidly in organisations around the world (Wall, 2005). This had led to a change in perspective, in terms of which the information security community has transitioned from a mere management-oriented stance to one of information security governance (ISACA, 2012a, p. 13, 2012b; S. Von Solms & Von Solms, 2008, p. iv; S. Von Solms, 2006). Accordingly, although information security management has not been eliminated completely, as management and governance are closely related yet distinguishable (refer to subsection 3.2.1, p. 63), it is no longer the primary focus.

Consequently, it is today commonly accepted that information security governance is a crucial component of successful business operations (S. Von Solms & Von Solms, 2008, p. iv). The information security community therefore now accepts that executive management plays a far greater role than merely providing commitment and should rather be involved directly in the security efforts (Institute of Directors in Southern Africa, 2009a, pp. 86–87).

Unfortunately the information security management framework of Vermeulen and Von Solms (2002) took the former stance; hence, the author of this work argues that this stance may no longer be sufficient for organisations, especially SMMEs, which are now becoming more heavily dependent on information and IT to run their business operations (Kankanhalli et al., 2003). The author therefore argues that the focus of the existing framework, shown in Figure 5.2 in relation to the direct–control action cycle of information security governance, which was primarily policy drafting and its upkeep by tactical and operational management, should be expanded to encompass the entire governance process.

The argument therefore stands that the direct and control actions of governance, as well as strategic-level management, should feature more prominently. Thus, executive management should not only provide commitment, but should also be actively involved in the information security governance process by establishing an information security strategic vision and, subsequently, board directives.

Similarly, the follow-up action should not only focus on the upkeep of information security policies, but should now also involve various other activities. These include the compliance analysis of security controls and policies and so on, in addition to the aggregation of the results of such analyses to the corporate information security policy, security requirements and board directives established by tactical-level management and sanctioned for by strategic level management.

Furthermore, as some SMMEs have little expertise and experience in implementing information security governance, the level of detail of the existing framework may be questionable. The author thus argues that far greater detail should be offered in order to assist SMMEs in their information security governance efforts. Hence, mention should be made of the tools that can be used and deliverables that can be expected at each management level in order to realise such governance. This should provide far greater assistance to these enterprises than merely indicating what components should be addressed.

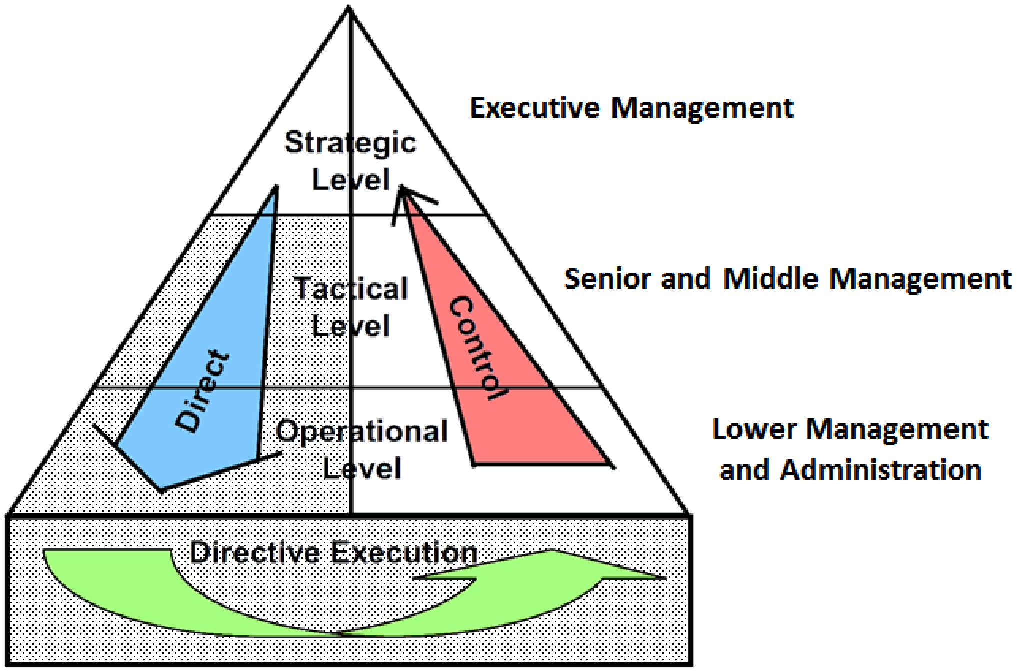
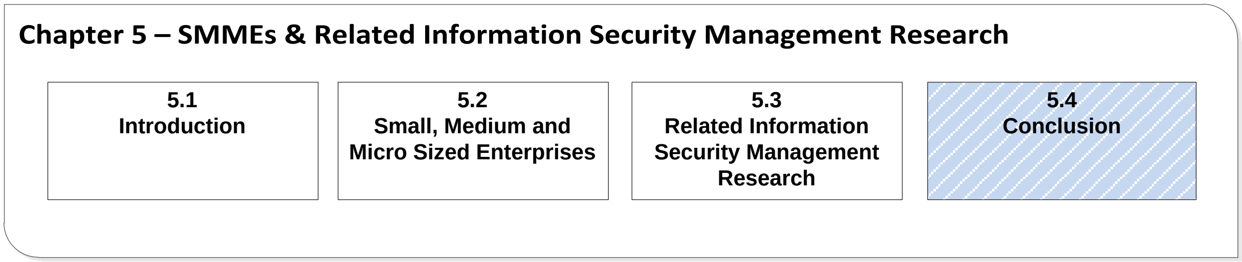


Figure 5.2 – Focus of the existing framework (shaded area)

The author of this work therefore argues, based on the above-mentioned statements, that the existing framework may exhibit properties that could make it unfeasible for use by SMMEs to address information security governance adequately. It therefore stands to reason that an information security governance framework, perhaps based on this existing framework, should be developed to alleviate the shortcomings mentioned in the existing framework. It is believed that such a framework would assist SMMEs further, since it would correspond with the current stance witnessed in the information security community.

To conclude, this section investigated research previously conducted that relates to this work, which aims at assisting SMMEs to address information security and its management. This research took the form of an information security management framework. Finally, it was found that this related research, given the vast change in the dependency on IT witnessed globally in conjunction with the requirement for proper information security governance, exhibits some inadequacies. Hence, it was argued that an information security governance framework should be developed to address these inadequacies.

5.4 Conclusion



Chapter 5 – SMMEs & Related Information Security Management Research

5.1 Introduction

5.2 Small, Medium and Micro Sized Enterprises

5.3 Related Information Security Management Research

5.4 Conclusion

The target audience of the forthcoming information security governance framework is SMMEs. Hence, a sound understanding of SMMEs and their importance, unique characteristics and information security challenges is necessary for its development. These topics were therefore described in this chapter.

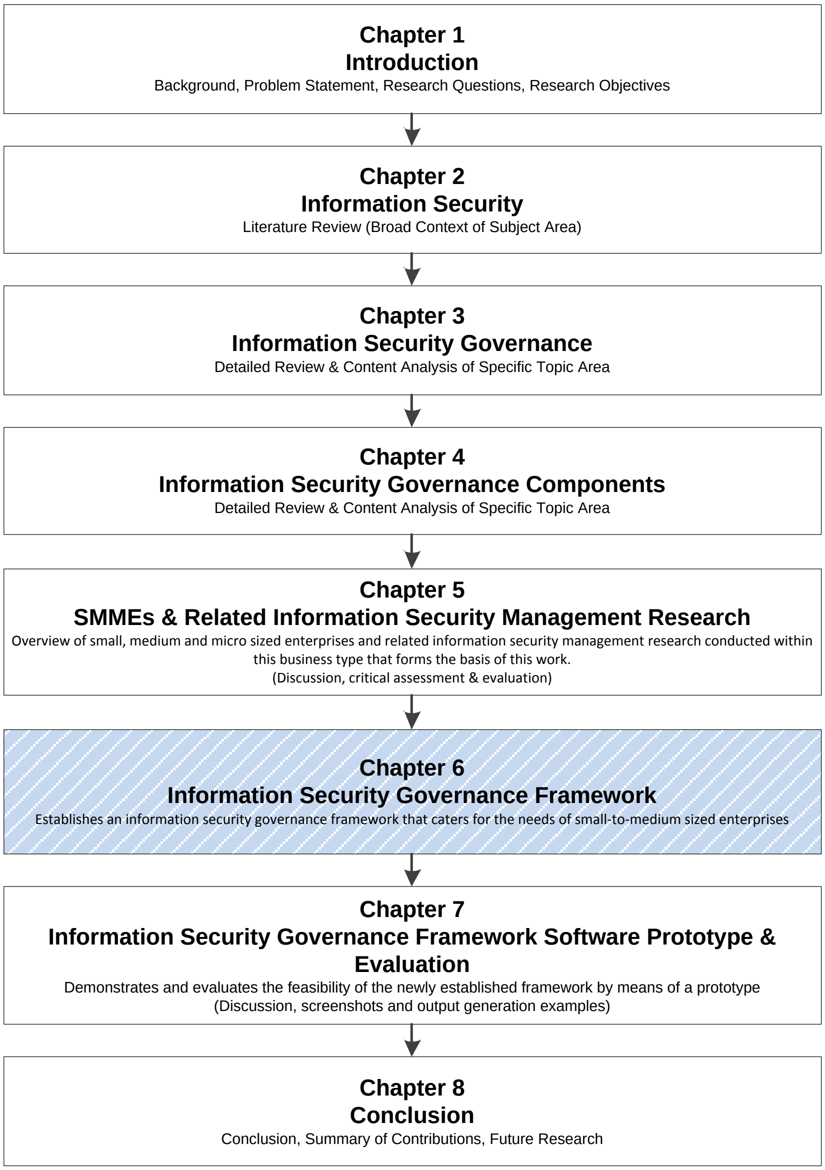
It was indicated that SMMEs are present in economies around the world (Sánchez et al., 2010) and have come to be essential for their innovation and flexibility (Koornhof, 2009, p. 28; Le Roux, 2010, p. iv). Further, it was mentioned that many nations have now started to introduce information technologies to these enterprises in order to afford them additional benefits, such as continued growth and competitiveness (Gupta & Hammond, 2005; Wall, 2005).

However, as the dependence on information and its supporting technologies increases, the importance of information protection should follow (ISO/IEC 27002, 2005, p. viii; S. Von Solms & Von Solms, 2008, p. 139). Unfortunately, it was shown that these enterprises often experience significant challenges in addressing such protection and therefore often have little or no security measures in place This is especially true of information security governance (Gupta & Hammond, 2005; Upfold & Sewry, 2005; Yildirim et al., 2010). Consequently, it was argued that these enterprises require significant assistance in this regard.

Subsequently, the reader was introduced to research relating to this work, which attempts to assist enterprises with managing information security properly. This related research took the form of an information security management framework (Vermeulen & Von Solms, 2002). It was, however, indicated that the vast change in the dependency on IT globally as well as the requirement for proper information security governance have caused some shortcomings to be identified. Consequently, it was argued that a modern-day information security governance framework should be developed. This forms the primary focus of the following chapter.

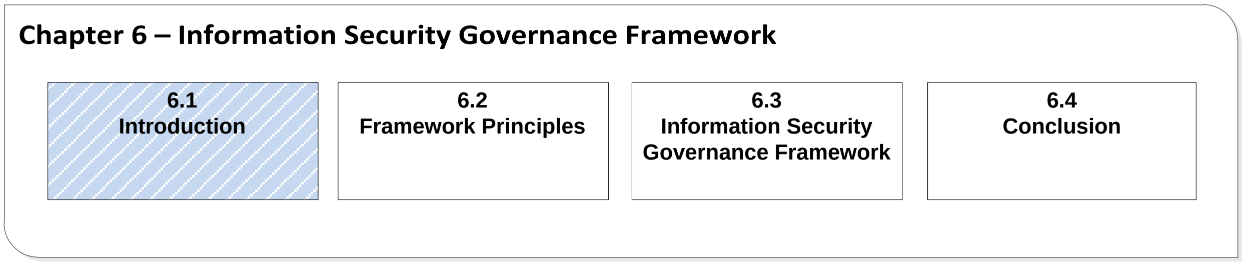
Chapter 6: Information Security Governance Framework

This chapter aims to introduce the reader to the information security governance framework that represents the solution to the research problem of this work. Firstly, the characteristics of a successful information security governance framework are established and, subsequently, this information security governance framework is depicted, by means of modelling techniques, and discussed.


Chapter 1
Introduction
Background, Problem Statement, Research Questions, Research Objectives
Chapter 2
Information Security
Literature Review (Broad Context of Subject Area)
Chapter 3
Information Security Governance
Detailed Review & Content Analysis of Specific Topic Area
Chapter 4
Information Security Governance Components
Detailed Review & Content Analysis of Specific Topic Area
Chapter 5
SMMEs & Related Information Security Management Research
Overview of small, medium and micro sized enterprises and related information security management research conducted within this business type that forms the basis of this work.
(Discussion, critical assessment & evaluation)
Chapter 6
Information Security Governance Framework
Establishes an information security governance framework that caters for the needs of small-to-medium sized enterprises
Chapter 7
Information Security Governance Framework Software Prototype & Evaluation
Demonstrates and evaluates the feasibility of the newly established framework by means of a prototype
(Discussion, screenshots and output generation examples)
Chapter 8
Conclusion
Conclusion, Summary of Contributions, Future Research

"It is the framework which changes with each new technology and not just the picture within the frame" – Marshall McLuhan (BrainyQuote, 2012a)

6.1 Introduction


Chapter 6 – Information Security Governance Framework
6.1 Introduction
6.2 Framework Principles
6.3 Information Security Governance Framework
6.4 Conclusion

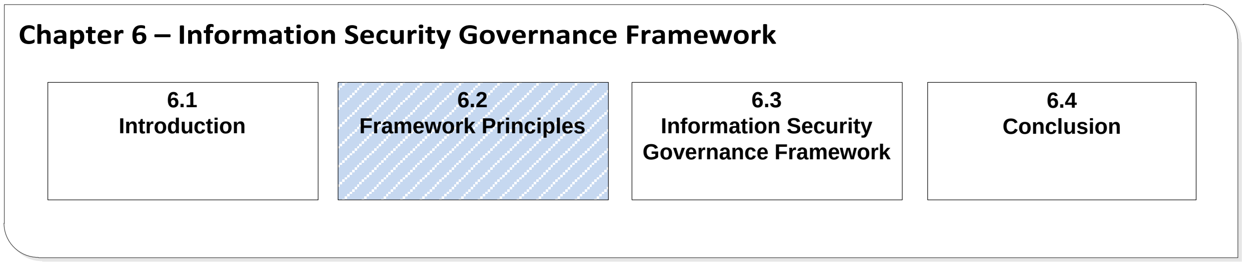
Organisations today are placing significant dependency on information and IT for successful business operations and prosperity (Wall, 2005). Consequently, organisations should take the necessary precautions to ensure that adequate protection is offered to safeguard this critical information and the technologies from harm (ISO/IEC 27002, 2005, p. viii). As the importance of information and IT and their protection increases in modern-day organisations, proper governance should also be ensured (S. Von Solms & Von Solms, 2008, pp. iv, 139). This is a vital duty of both strategic-level management and every other employee of the organisation, especially if strategic-level management is to address its corporate governance obligations (Institute of Directors in Southern Africa, 2009a, pp. 86–87).

Information security governance necessitates the employment of various components to facilitate both the directing and the controlling of information security in an organisation. These components include board directives, information security policies, compliance analysis and many more (S. Von Solms & Von Solms, 2008, p. 74). Unfortunately, SMMEs, which are the target audience of the forthcoming framework, often experience a lack of resources and expertise, which places a significant burden on them when attempting to address these information security governance components properly (Koornhof, 2009, pp. 82–83; Yildirim et al., 2010). Consequently, literature suggests that these enterprises often have little or no information security governance measures in place (Gupta & Hammond, 2005; Upfold & Sewry, 2005; Yildirim et al., 2010).

To aid these enterprises in this challenge, much research has been conducted over the years (Coertze et al., 2011; Hoppe et al., 2002; Vermeulen & Von Solms, 2002). Of specific interest to this work is research that took on the form of an information security management framework (Vermeulen & Von Solms, 2002), as well as a working prototype that originated from the study (Hoppe et al., 2002). Unfortunately, given the vast change in the dependency on IT witnessed globally as well as the requirement for proper information security governance, some shortcomings have been identified with these artefacts (Coertze et al., 2011). Consequently, it is argued that in order to address the current information security issues being experienced worldwide by SMMEs, a modern-day information security governance framework should be developed to address the inadequacies of this research. This then forms the primary objective of this chapter.

The above-mentioned information security governance framework will be detailed in this chapter as follows: Firstly, the principles that should be exhibited by the forthcoming framework, given the previously discussed literature, will be deliberated to offer a detailed understanding. Secondly, the framework combined with a detailed discussion of its workings will be introduced. Finally, a discussion of the benefits which originate from the framework will follow.

6.2 Framework Principles


Chapter 6 – Information Security Governance Framework
6.1 Introduction
6.2 Framework Principles
6.3 Information Security Governance Framework
6.4 Conclusion

Before the information security governance framework can be presented, its principles should be clearly understood. Hence, based on the previously discussed literature, a series of principles will now be established.

S. Von Solms and Von Solms (2008, pp. 3–4) state that all forms of governance, in particular information security governance, should exhibit a distinctive direct–control action cycle (refer to subsection 3.2.3.3, p. 73). This cycle generally consists of three actions, namely: the *direct*, *control* and *execute* actions. It is thus essential that the forthcoming framework, which addresses information security governance, use this action cycle as its basis and clearly depict it in its process flow. Hence, the *direct*, *execute* and *control* actions should be clearly discernible in the framework.

Information security governance requires not only strategic-level management to be involved, but also all the other levels of management. This is clearly indicated by S. Von Solms and Von Solms (2008, p. 3), who suggest that three broad levels of management can generally be observed as operating within an organisation, namely, the strategic-, tactical- and operational-level management (refer to subsection 3.2.3.3, p. 73). They further indicate that all three of these levels of management have specific duties to fulfil during the successful implementation and continued operation of information security governance. Thus, it is vital that the forthcoming framework clearly indicate the involvement of these management levels as well as their respective obligations in the information security governance implementation and process.

Strategic-level management should not only display commitment towards the information security governance efforts, but should also play a critical role in it (R. Von Solms & Von Solms, 2006b). This involvement is essential if information security is to be aligned with the IT and business goals of an organisation (ISACA, 2012b, p. 13). Consequently, this involvement is often shown to be one of the first things that is sought when initiating the *direct* action (R. Von Solms & Von Solms, 2006a). The forthcoming framework should therefore clearly exhibit this involvement by strategic-level management.

When focusing specifically on the *direct* action of information security governance, strategic-level management should also clearly indicate its vision and strategy for information security in an organisation (S. Von Solms & Von Solms, 2008, p. 42). This is vital if a successful information security governance programme is to be initiated and subsequently implemented, since the vision and strategy will have a direct impact on the motivation for the programme and that of the rest of the organisation. The vision and strategy established by strategic-level management will therefore further impact all the information security governance efforts that follow. Note that this vision and strategy are commonly captured by means of board directives (refer to subsection 4.2.3, p. 112). Consequently, it is vital that the forthcoming framework should clearly indicate that it is strategic-level management's task to establish these directives.

Subsequent to the establishment of these board directives, it is vital that the applicable security requirements of the organisation be identified (ISO/IEC 27002, 2005, p. ix). Factors that should be considered during the establishment of security requirements include regulatory requirements and risks (both internal and external) to the organisation linked to the business requirements (R. Von Solms et al., 2011). It should be noted that the security requirements of an organisation have a direct impact on the remainder of the information security governance implementation. Hence, it is essential that the identification and establishment of security requirements should be clearly indicated in the forthcoming framework.

Following the establishment of security requirements, the next phase involves the development of the information security policy architecture (refer to subsection 4.2.2, p. 110). This architecture, as previously mentioned, consists of various documents, which have to be drafted. The drafting of the corporate information security policy (refer to subsection 4.2.4.1, p. 115), which is typically drafted by tactical-level management and approved by strategic-level management, indicates the starting point of this process (Bacik, 2008, p. 47). The corporate information security policy will usually contain, among other things, details of strategic-level management's vision and strategy for information security, as well as the information security duties of all parties in the organisation (ISO/IEC 27002, 2005, p. 7; S. Von Solms & Von Solms, 2008, p. 77).

The corporate information security policy is generally supported by various secondary-level policies (refer to subsection 4.2.4.2, p. 118) and security procedures (refer to subsection 4.2.5, p. 120). During the drafting of company standards, a type of secondary-level policy drawn up by tactical-level management, security controls (refer to subsection 2.3.4, p. 52) will typically be selected from international information security standards (refer to subsection 2.3.2, p. 40) or other credible sources. These selected controls will in turn form the information security benchmark that will be upheld in the organisation (R. Von Solms & Von Solms, 2006a).

However, this corporate information security policy and secondary-level policies generally offer little detail on the way in which the selected security measures should be used and implemented; hence they are typically supported by several security procedures. These are drawn up by operational-level management for the use of operational staff.

It is thus essential that the forthcoming framework should show the establishment of the information security policy architecture, that is, the drafting of a corporate information security policy, supporting secondary-level policies and security procedures. Furthermore, the process of security control selection from information pertaining to international security standards or other credible sources should also be clearly indicated.

Focusing specifically on the *control* action of information security governance, it is essential that the measures implemented for information security and its governance are complied with and adhered to (R. Von Solms & Von Solms, 2006a). Hence, it is important that measures be put in place to evaluate and capture the compliance being achieved as well as taking corrective action if compliance is unsatisfactory. The *control* action therefore focuses specifically on measuring compliance with the documentation and security measures introduced during the *direct* action.

Typically, the *control* action is initiated by operational-level management which carries out a compliance analysis exercise with the support of various operational and IT staff (refer to subsection 4.3.1, p. 123). The outcome of this exercise should in turn be submitted to tactical-level management. However, the outcome of this exercise should be further conveyed from tactical-level management to strategic-level management so as to allow this level of management to evaluate and adjust the vision and strategy for information security if necessary (R. Von Solms & Von Solms, 2006a). Hence, it is essential that this compliance analysis exercise be clearly indicated in the forthcoming framework as well as the aggregation process stated above that originates from operational-level management and is escalated to strategic-level management

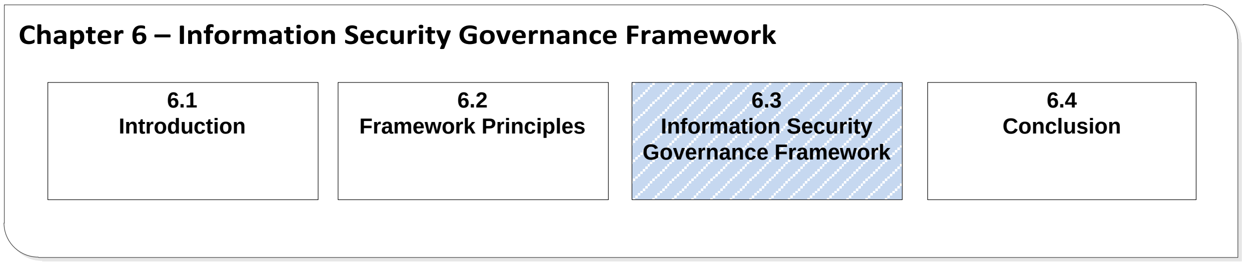
Finally, as strategic-level management is never above reproach, it too should evaluate its own information security governance efforts (R. Von Solms & Von Solms, 2006b). Accordingly, a clear indication can be obtained of whether this management level is approaching and addressing information security governance with due care and due diligence. It is thus essential that the involvement of this level be evaluated (refer to subsection 4.3.2, p. 125) and such an evaluation exercise should be clearly indicated in the envisaged framework, as well as the due care and due diligence indicator that it can offer.

In summary, the principles that should be exhibited by the forthcoming framework include the following:

- Direct–control action cycle depiction
    - *direct*, *control* and *execute* action representation
- Management levels and duties illustration
- Strategic-level management involvement portrayal
- *Direct* action delineation
    - the development of board directives
    - the establishment of security requirements
    - the development of the information security policy architecture
        - the drafting of the corporate information security policy
        - the drafting of supporting secondary-level policies
        - the drafting of security procedures
        - the selection of security controls
- Control action delineation
    - the execution of a compliance analysis exercise
    - the depiction of the compliance analysis exercise results aggregation
    - the execution of an executive involvement evaluation or similar concept.

These principles were subsequently used to develop an information security governance framework, which addresses and alleviates the previously identified shortcomings in the information security management framework established by Vermeulen and Von Solms (2002). An introduction to this framework as well as a thorough discussion of its detailed workings follows in the next section.

6.3 Information Security Governance Framework


Chapter 6 – Information Security Governance Framework
6.1 Introduction
6.2 Framework Principles
6.3 Information Security Governance Framework
6.4 Conclusion

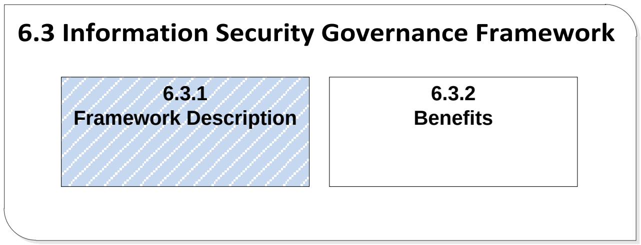
A framework is defined as “the basis for something being constructed” (*American Heritage Dictionary*, 2011). A framework, like an architectural plan, is “a set of assumptions, concepts, values, and practices” (*American Heritage Dictionary,* 2011) that constitutes a way of viewing the fundamental structure of a system (*Oxford Dictionary*, 2010). As such, it is often used to specify the essential aspects of a proposed system or product (Olivier, 2009, p. 45). Some of these aspects may include (Macaulay, 2004):

- the components of the system
- the relationship between these components
- the principles that govern the “evolution and design” of the system.

Frameworks are therefore used as blueprints when designing new systems or products. Consequently, the goal of the envisaged framework is to act as a guide for organisations, in particular SMMEs that wish to implement or improve an information security governance system.

Having defined the purpose of a framework along with the goal of the envisaged framework, the principles (refer to section 6.2, p. 152) were used as guidelines for developing an information security governance framework. A detailed discussion of the components, relationships and workings of this framework follows in the next subsection.

6.3.1 Framework Description



The information security governance framework (see Figure 6.1) uses as its basis the direct–control action cycle for information security governance as outlined by S. Von Solms and Von Solms (2006a; 2008, pp. 3–4). This was shown to be a principle, as previously discussed.

Information security governance operates on all three levels of management, namely, the strategic, tactical and operational levels (R. Von Solms & Von Solms, 2006a). Hence, according to the principle of *management levels and duties illustration*, these three levels are clearly indicated in the framework as the primary layers and form the focus for separation. This is of specific interest as each management level requires different aspects to be produced and monitored in line with its duties, in order for proper information security governance to be present.

Similarly, the three actions of governance, namely, *direct*, *execute* and *control,* are also depicted in the composition of the framework, in line with the principle of *direct, control and execute action representation*. These three actions are shown to support each other and each is reinforced by tooling recommendations and input/output indicators. These recommendations and indicators are viewed as essential when giving guidance to organisations on the way each action can be realised.

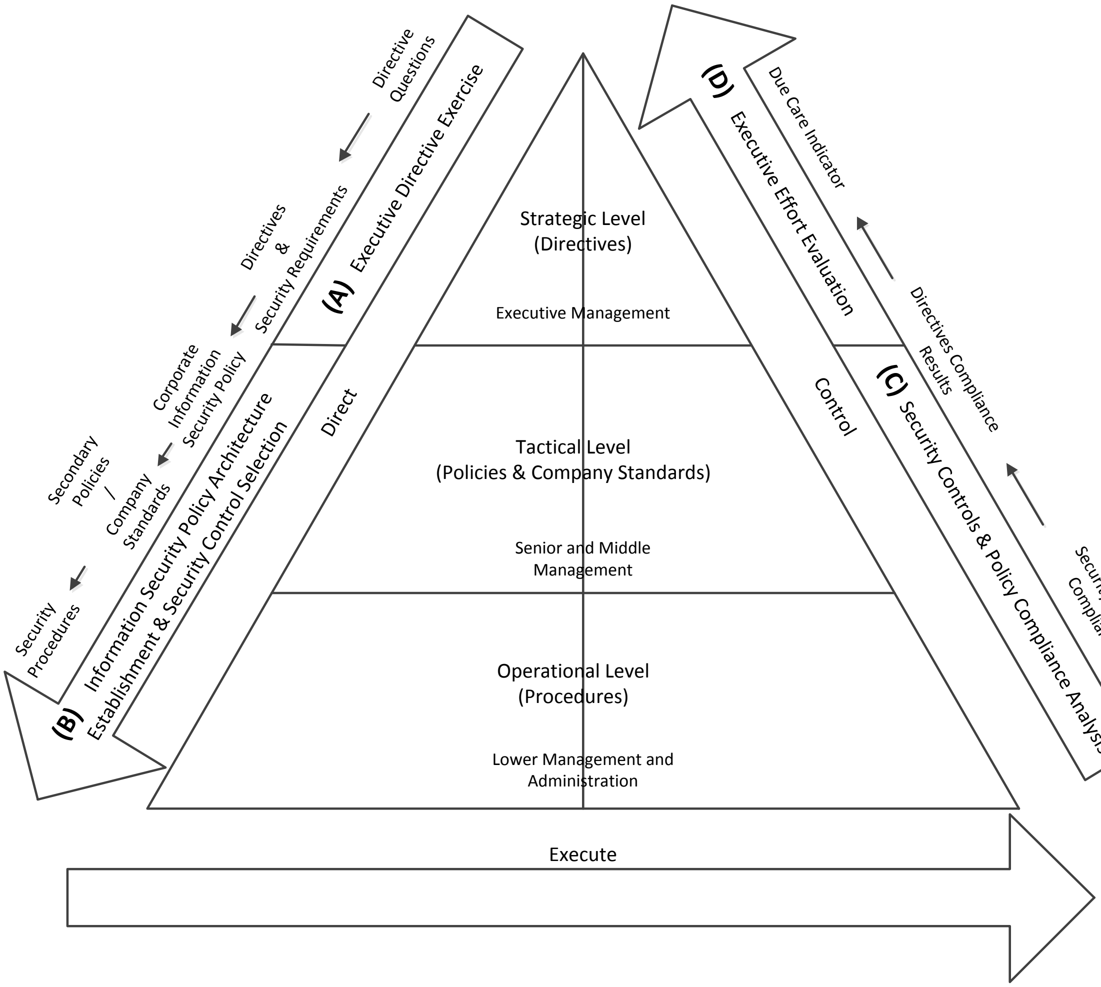
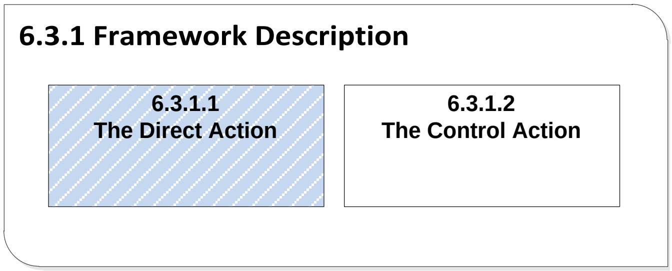


Figure 6.1 – The information security governance framework

6.3.1.1 The Direct Action



Executive Directive Exercise

According to international standards and best practices for information security governance, strategic-level management must take responsibility for the direction and control of information security (ISACA, 2012a, p. 14; ISO/IEC 27002, 2005, p. 9; Institute of Directors in Southern Africa, 2009a, pp. 86–87). Directing starts with strategic-level management, where it should be clearly indicated how important the information assets are and how they contribute to the strategic vision of the company (S. Von Solms & Von Solms, 2008, p. 42). This is typically captured in board directives and, when captured, should be based on factors that originate from various sources.

Various resources exist that offer guidance for strategic-level management when deliberating these factors and establishing board directives. One example is the book *"Information security governance: Guidance for boards of directors and executive management"* (Brotby, 2006). The framework emanating from this work facilitates the use of such resources by stating that an executive directive exercise should be conducted. This can raise a series of thought-provoking information security-related questions (or directive questions) for assessment by executive management (as indicated by **(A)** in Figure 6.1, p. 159). One example of questions that may be posed for executive management in this regard may be viewed in Addendum D (p. 231). By applying the answers given in this exercise, board directives may be inferred from each of the questions asked (refer to Addendum E, p. 233). The output of such an exercise is a set of clearly defined board directives that satisfies the principles of *strategic-level management involvement portrayal* and *the development of board directives*. These directives reflect strategic-level management's expectations and become the input for the other management levels. In this way, these directives contribute to the security requirements of the organisation.

Security Requirements Establishment

In an organisation it is vital that strategic-level management, or even tactical-level management, should determine the applicability and appropriate levels of security requirements (ISO/IEC 27002, 2005, p. ix). These may include, but are not limited to the availability, integrity, confidentiality, auditability and authentication of information assets (Gerber & Von Solms, 2001; Vermeulen & Von Solms, 2002). The existing information security management framework (Vermeulen & Von Solms, 2002) already supports the establishment of such security requirements; hence this is also discernible in this framework. It should, however, be noted that various approaches can be used to establish security requirements; these can include performing a risk analysis (refer to subsection 2.3.3.3, p. 48) or a security requirements analysis exercise (Gerber, Von Solms, & Overbeek, 2001) among others. This framework does not, however, prescribe a specific approach to be used, but rather indicates that security requirements should simply be established using an applicable tactic. This then satisfies the principle of *the establishment of security requirements*. Also visible in the framework is the fact that the board directives that emanate from strategic-level management should also have an impact on these security requirements. As a result, the outcome of the risk analysis exercise, the security requirements analysis exercise or other approach, together with the board directives, should influence the security requirements. Once established, these security requirements govern the content of the documents used by tactical and operational-level management when forming the information security policy architecture (S. Von Solms & Von Solms, 2008, pp. 74–75).

ISPA Establishment and Security Control Selection

Corporate Information Security Policy

As already mentioned, the initiation of information security policy architecture formation is typically indicated by tactical-level management's drafting of the corporate information security policy, which is also indicated by this framework. The corporate information security policy can be seen as the cornerstone policy that defines all the high-level security statements applicable to the business (Bacik, 2008, p. 47). Typically, the corporate information security policy will reiterate strategic-level management's board directives, set the scope of the security effort, specify security roles and specify the vision for the security concerns of the business (S. Von Solms & Von Solms, 2008, p. 77). As can be seen from the framework, the corporate information security policy should be supported by various secondary-level policies, in particular company standards, which offer further detail and should be aligned to the security policy.

Secondary-Level Policies/Company Standards

Company standards detail the operational security measures that will be implemented in an organisation (refer to subsection 4.2.4.2, p. 118). Generally, such operational security measures are selected from international standards or best practices, such as ISO/IEC 27002 (2005), which offers specific guidance on the security controls that can be considered for implementation. Typically, the selection and applicability of operational security measures are directly related to the identified security requirements, the type of business and the current observed situation as far as information security is concerned. It should, however, be noted that company standards typically do not include information on procedures and should therefore be supported by security procedures as indicated by the framework.

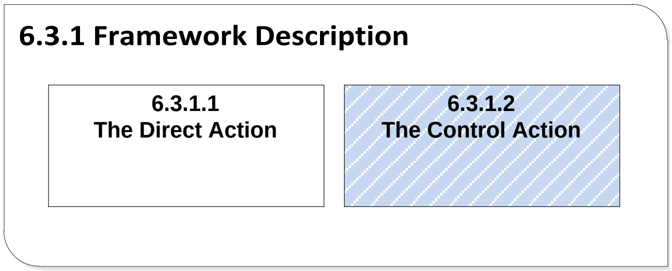
Security Procedures

Security procedures generally guide operational staff in the realisation of the security measures stipulated in an organisation’s company standards (R. Von Solms et al., 2011). They characteristically contain statements that can be applied in the day-to-day operations of the organisation (Coertze et al., 2011). Business operations therefore depend heavily on these procedures to ensure that a safe and secure environment is maintained. Hence, the drafting of security procedures is also included in this framework.

The process of identifying security requirements and drafting the corporate information security policy and company standards in addition to security procedures has previously been indicated in Vermeulen and Von Solms’s (2002) information security management framework. Consequently, it has been included in this framework (as indicated by **(B)** in Figure 6.1, p. 159) as well so as to address the principle of *the development of the information security policy architecture*.

The framework therefore also clearly depicts the *direct* action of information security governance, as well as the components that should be implemented during its realisation. This subsequently satisfies the principle of *direct action delineation*.

6.3.1.2 The Control Action



However, the security measures implemented during the *direct* action do not necessarily guarantee voluntary compliance and adherence; therefore the action of continuous *control*, or *compliance monitoring and evaluation*, is vital (R. Von Solms & Von Solms, 2006a). This is clearly indicated in the framework.

Satisfactory levels of information security can be preserved at the operational level with a combination of two things. Firstly, the security controls, or operational measures, selected and implemented in the organisation have to be monitored for efficiency and effectiveness (ISO/IEC 27002, 2005, p. 6). Secondly, the company standards and security procedures established have to be evaluated in terms of their use by operational staff and the extent to which staff adhere to them (R. Von Solms & Von Solms, 2006a).

Policy and Company Standards Compliance Analysis

The *control* action is typically initiated at the level of operational management, where a compliance analysis exercise (refer to subsection 4.3.1, p. 123) may be performed based on the established security controls and company standards (as indicated by **(C)** in Figure 6.1, p. 159). This compliance analysis exercise typically involves a questionnaire based on the auditing guidelines and questions prompted by the international information security standards and best practices, such as ISO/IEC 27001 (2005). A questionnaire of this nature will typically present a series of security control-related questions to both operational and tactical levels of management in order to evaluate the implementation, effectiveness and efficiency of the security measures stipulated in an organisation's company standards. This may be further supported by observational or interview information, which can provide an indication of whether operational and IT staff are adhering to the prescribed security procedures. The outcome of this exercise will, in turn, give an indication of the compliance achieved in terms of company standards and security measures. Thus, by identifying this compliance analysis exercise in the framework, the principle of *the executive of a compliance analysis exercise* is met.

It may be worth mentioning that other electronic discovery (e-discovery) methods, such as log file interpretation or the Compliance Management Approach (S. Von Solms & Von Solms, 2008, pp. 98–105) amongst others, could be used in addition or per replacement of the above-mentioned compliance analysis exercise to determine the level of policy and security control compliance. Unfortunately these methods may prove to be too complex or technical in nature for use by some SMMEs, as they require extensive expertise and knowledge of the IT systems and information security mechanisms present within the enterprise.

It is, however, important to realise, irrespective of the approach used, that the results of such a compliance analysis exercise or other method should not only be used for the correction of ineffective, inefficient or unimplemented security controls by operational-level management, but should also be aggregated to the upper management levels for decision making, strategizing, reporting and benchmarking (as a baselining exercise) (R. Von Solms & Von Solms, 2006a). To facilitate the decisions of strategic-level management, this level of management needs to receive a frequent aggregated report on the current information security situation in the organisation. Furthermore, it also needs to obtain an indication of whether its board directives are being met. Thus, this process of result aggregation is clearly discernible in the *control* action process flow shown in the framework. Also note how the framework suggests that the aggregated results are used at each individual management level to evaluate and compare the measures applied when fulfilling its *direct* action duty. The depiction of this aggregation process thus ensures that the principle of *the depiction of compliance analysis aggregation* is satisfied.

Executive Involvement Evaluation

Finally, strategic-level management, that is, the executive management of the organisation, should also be active in determining its own compliance with legislation, regulations and best practices (R. Von Solms & Von Solms, 2006b). This is because executive management is never beyond reproach, and it is its duty to ensure that any measures taken allow for the continued prosperity and growth of an organisation (Institute of Directors in Southern Africa, 2009a, pp. 22–47). The framework therefore specifies that strategic-level management should actively ensure that it is taking due care and due diligence with regard to information security governance. This can be achieved by conducting an executive involvement evaluation exercise (as indicated by **(D)** in Figure 6.1, p. 159), where a checklist, such as the one established by R. Von Solms and Von Solms (2006b), could be completed by this level of management to evaluate the extent to which it fulfils its duties with regard to proper information security governance. It should, however, be noted that the framework is not prescriptive in this regard; thus other methods may also be used to assess this requirement. It is nevertheless important to note that, whatever the method used, it should be able to give strategic-level management an indication of any mismanagement or where it may be at risk of prosecution. In the framework, this is referred to as the due care indicator; this also denotes the end of the *control* action. This executive involvement evaluation and the due care indicator, as included in the framework, mean that the principle of *the execution of an executive involvement evaluation exercise or similar concept* has thus been met.

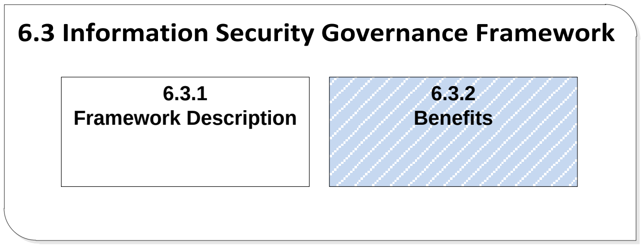
This process of operational-level management performing a compliance analysis exercise, aggregating the results to the upper management levels and strategic-level management performing an executive involvement evaluation exercise is denoted in this framework as constituting the *control* action of information security governance. Consequently, the principle of *control action delineation* is also addressed.

It should also be noted that S. Von Solms and Von Solms (2008, p. 46) state that the direct–control action cycle is not a once-off process, but rather a recurring loop. Therefore, the *direct*, *execute* and *control* actions may reoccur continuously throughout organisations' lifetimes, as new information assets or technologies are introduced and new security threats identified. Consequently, arrows are used in the framework to indicate this circular flow.

As is evident from the above discussion, the information security governance framework acts as a guide for organisations, in particular SMMEs, when implementing or improving an information security governance system. The framework does this by providing actionable information on the components and processes that constitute and/or support the implementation of proper information security governance in an organisation.

As some organisations are neither aware nor knowledgeable of the above-mentioned components and processes (Koornhof, 2009, p. 83; Yildirim et al., 2010), this framework offers significant benefits when addressing and possibly alleviating this problem. The following subsection details some of the benefits that may be associated with this framework.

6.3.2 Benefits



The establishment of the information security governance framework holds many benefits for both organisations and the information security community. This subsection highlights the benefits that this framework add as a result of its principles, as well as identifying the way it enhances the existing information security management framework established by Vermeulen and Von Solms (2002).

The information security governance framework affords many benefits above and beyond those offered by the previously established information security management framework (Vermeulen & Von Solms, 2002). The vast change witnessed globally in the dependency on information and IT in organisations (Koornhof, 2009; Wall, 2005) has resulted in an increased requirement for proper information security governance to be addressed and adequately implemented (S. Von Solms & Von Solms, 2008, p. 139). However, the previously information security management framework (Vermeulen & Von Solms, 2002) merely addressed information security management, as discussed in subsection 5.3.2 (p. 145). Hence, it can be argued that this may no longer be sufficient for guiding organisations in this regard. Consequently, the information security governance framework offers a significant benefit because it specifically addresses information security governance while still retaining many of the vital concepts depicted in the previously established management framework. The change in framework focus is illustrated by a comparison, which is illustrated in Figure 6.2. Furthermore, the information security governance framework specifically addresses the critical success factors (see subsection 3.4.3.2, p. 99) and implementation steps (see subsection 3.4.3.3, p. 100) of information security governance. Thus it offers SMMEs a steadfast foundation for their information security governance implementation, which adheres to international best practices and principles.

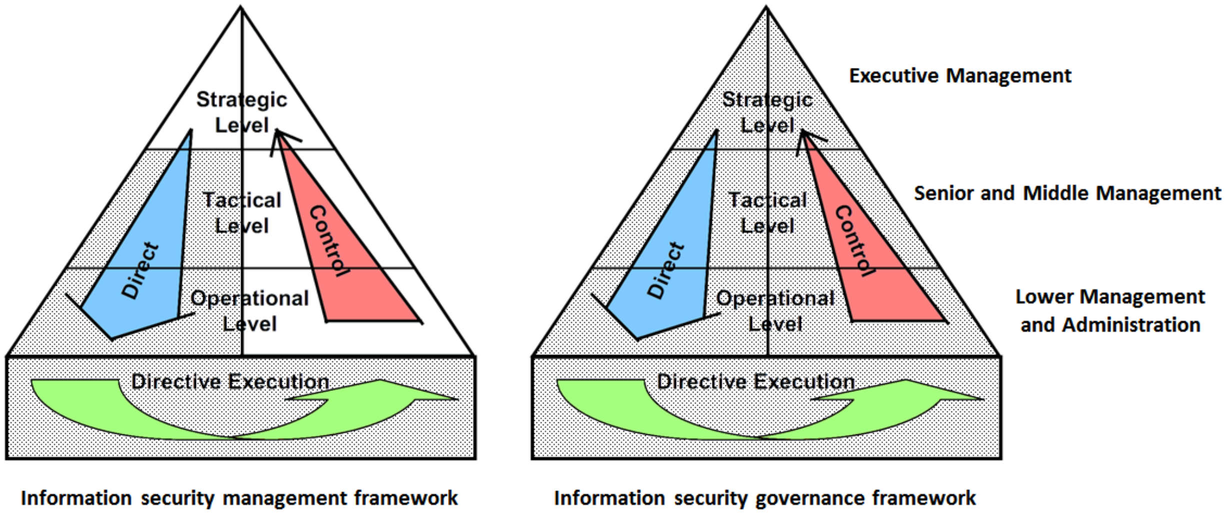


Figure 6.2 – Comparison of framework focus (shaded area)

One of the shortcomings of the original information security management framework (Vermeulen & Von Solms, 2002) was that the *direct* and *control* actions of governance did not feature prominently in its depiction. Although many of the components that typically constitute the *direct* action were clearly indicated, the *control* action was merely mentioned. Hence, the new framework offers a significant benefit in that it details the entire direct–control action cycle and subsequently each individual action. Furthermore, it offers specific details on the way each of these actions can be realised, thus offering greater insight into the components and processes that should be implemented.

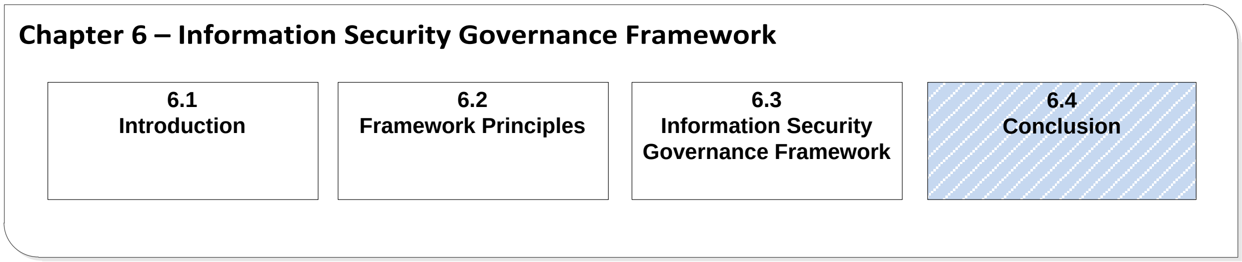
Similarly, strategic-level management did not feature prominently in the previous framework. Thus, executive management might have been tempted to believe that they should only show commitment to information security (as was shown in the existing framework, refer to subsection 5.3.1, p. 142). This was, however, demystified in the new framework, as it indicates that this level of management should be actively involved in the information security governance process by establishing an information security strategic vision and, subsequently, information security board directives (S. Von Solms & Von Solms, 2008, p. 76). This is indicated by means of a strategic-level management layer in the core of the framework as well as an indication that board directives should be established and that strategic-level management should also evaluate its own information security efforts for due care and due diligence.

Likewise, it was argued that the existing management framework's *follow-up* or *control* action focused only on the maintenance of information security policies, therefore information security governance should also involve other activities. These include a compliance analysis of security controls, policies and so on, as well as the aggregation of the evaluation results to the corporate information security policy, security requirements and security board directives established by tactical-level management and sanctioned by strategic-level management (R. Von Solms & Von Solms, 2006a; S. Von Solms & Von Solms, 2008, pp. 91–106). Consequently, the information security governance framework offers a significant benefit in that it clearly depicts the activities and components that should be implemented and/or used during the *control* action of information security governance.

Furthermore, as some organisations have little expertise and experience in implementing information security governance (Koornhof, 2009, pp. 82–83; Yildirim et al., 2010), the detail level of Vermeulen and Von Solms's (2002) framework was shown to be questionable. It is therefore argued that far greater detail should be offered if SMMEs are to be assisted properly in their information security governance efforts. Hence, the information security governance framework offers a significant benefit in that it clearly makes mention of the tools and deliverables that can be used and should be expected at each management level. It is believed that this will be of great help to these organisations.

It can therefore be concluded that the establishment of the information security governance framework holds many benefits, not least because it enhances the existing information security management framework established by Vermeulen and Von Solms (2002). However, it should be noted that many more benefits could possibly emanate from the implementation or use of this framework, which is aimed at the development of an automated or semi-automated software application that targets information security governance implementation in SMMEs.

6.4 Conclusion


Chapter 6 – Information Security Governance Framework
6.1 Introduction
6.2 Framework Principles
6.3 Information Security Governance Framework
6.4 Conclusion

In the introduction to this dissertation the primary objective of this work was described as the establishment of a framework that could facilitate the implementation of sound information security governance principles in organisations with limited resources and expertise. With the establishment of the information security governance framework (see Figure 6.1, p. 159), this has been achieved.

This chapter introduced the reader to the principles of the framework, which became evident from the literature that was discussed. In summary, these principles included the following:

- Direct–control action cycle depiction
    - direct, control and execute action representation
- Management levels and duties illustration
- Strategic-level management involvement portrayal
- Direct action delineation
    - the development of board directives
    - the establishment of security requirements
    - the development of the information security policy architecture
        - the drafting of the corporate information security policy
        - the drafting of supporting secondary-level policies
        - the drafting of security procedures
        - the selection of security controls
- Control action delineation
    - the execution of a compliance analysis exercise
    - the depiction of compliance analysis exercise results aggregation
    - the execution of an executive involvement evaluation exercise or similar concept.

Subsequently, the framework was introduced as well as a detailed discussion of its components and finer workings. Further, specific mention was made of how the principles were addressed in the framework.

Afterwards, the benefits provided by this framework were highlighted. These benefits have accrued from the enhancements that were made to the existing information security management framework established by Vermeulen and Von Solms (2002), in addition to the realisation of the principles. These benefits include the following:

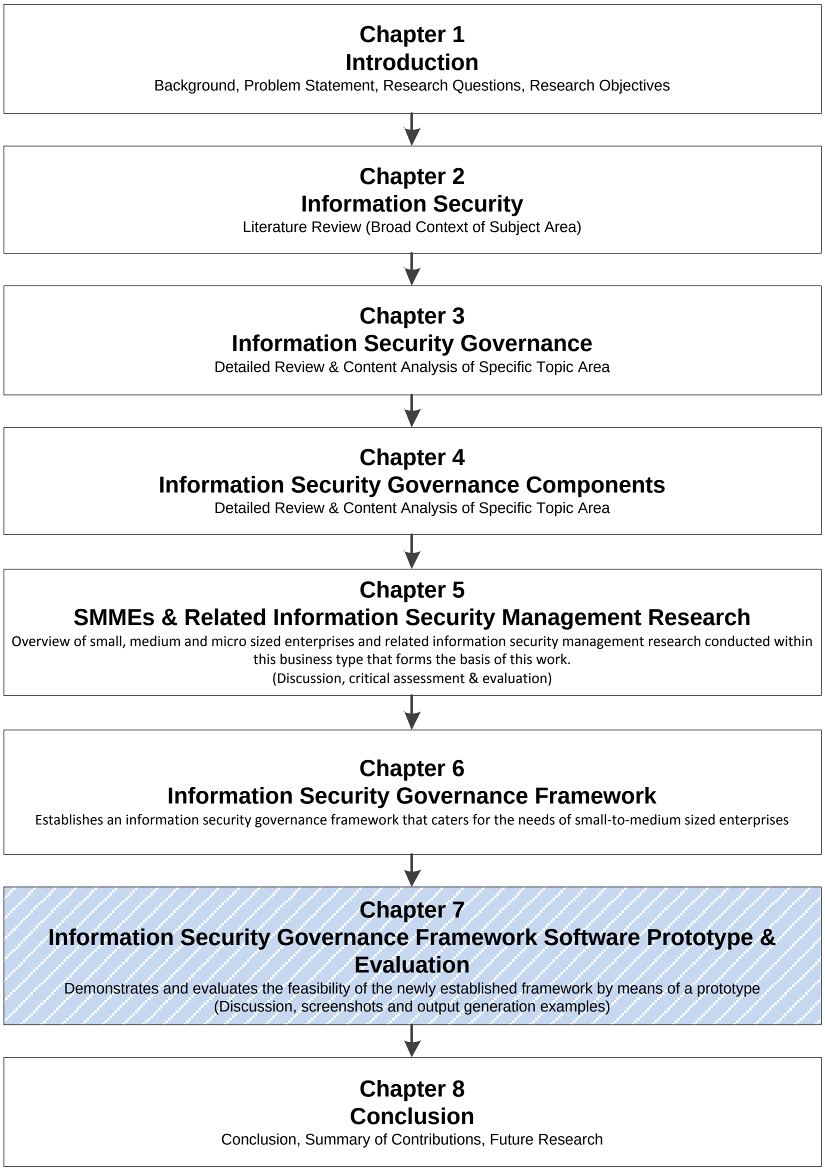
- transference of focus from information security management to governance
- inclusion of the critical success factors and implementation steps of information security governance
- specific mention of strategic-level management involvement in the information security governance process
- identification of the duties of the different management levels
- representation of the direct–control action cycle and its components for realisation in the follow-up or control action.

Furthermore, as some organisations have little expertise and experience in implementing information security governance (Koornhof, 2009, pp. 82–83; Yildirim et al., 2010), it was indicated that the framework’s level of detail would be beneficial as the tools that can be used and the deliverables that can be expected at each management level in an organisation are clearly spelt out.

It was nevertheless emphasised that countless more benefits may accrue from the implementation or use of this framework for information security governance implementation in SMMEs. Consequently, the development of a proof-of-concept software prototype, in order to illustrate the feasibility of this framework, forms the primary objective of the following chapter.

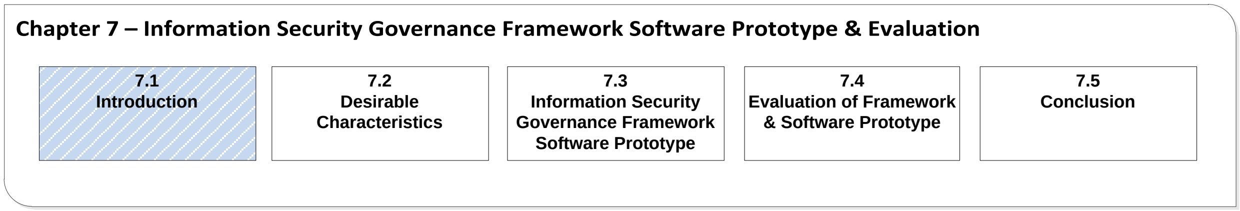
Chapter 7: Information Security Governance Framework Software Prototype and Evaluation

This chapter aims to demonstrate and evaluate the feasibility of the information security governance framework by means of a proof-of-concept software prototype targeted at SMMEs.


Chapter 1
Introduction
Background, Problem Statement, Research Questions, Research Objectives
Chapter 2
Information Security
Literature Review (Broad Context of Subject Area)
Chapter 3
Information Security Governance
Detailed Review & Content Analysis of Specific Topic Area
Chapter 4
Information Security Governance Components
Detailed Review & Content Analysis of Specific Topic Area
Chapter 5
SMMEs & Related Information Security Management Research
Overview of small, medium and micro sized enterprises and related information security management research conducted within this business type that forms the basis of this work.
(Discussion, critical assessment & evaluation)
Chapter 6
Information Security Governance Framework
Establishes an information security governance framework that caters for the needs of small-to-medium sized enterprises
Chapter 7
Information Security Governance Framework Software Prototype & Evaluation
Demonstrates and evaluates the feasibility of the newly established framework by means of a prototype
(Discussion, screenshots and output generation examples)
Chapter 8
Conclusion
Conclusion, Summary of Contributions, Future Research

“A pinch of probability is worth a pound of perhaps” – James Thurber (Quotes Star, 2012).

7.1 Introduction

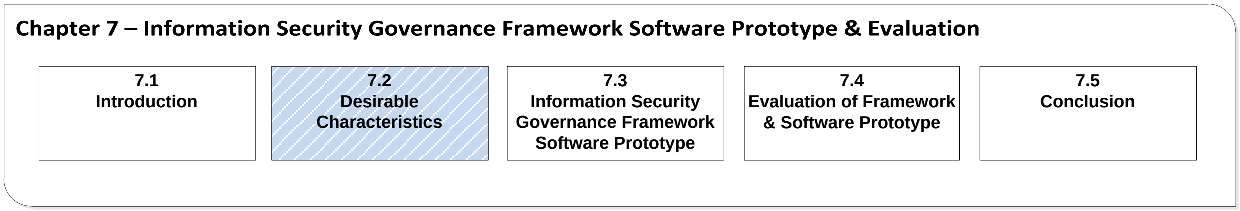

Chapter 7 – Information Security Governance Framework Software Prototype & Evaluation
7.1 Introduction
7.2 Desirable Characteristics
7.3 Information Security Governance Framework Software Prototype
7.4 Evaluation of Framework & Software Prototype
7.5 Conclusion

This research established an information security governance framework (shown in Figure 6.1, p. 159) that can facilitate the implementation of sound information security governance principles in organisations with limited resources and expertise. Although this framework provides many benefits, it was argued that it could offer countless more if used to implement an automated or semi-automated software application. This is especially true if used by SMMEs to implement information security governance efforts and address any related challenges.

Consequently, a proof-of-concept software prototype was developed to demonstrate such an implementation. The development of this prototype serves as an attempt to demonstrate the feasibility of the information security governance framework.

This information security governance framework software prototype will be detailed in this chapter as follows: Firstly, the desirable characteristics that governed its development and that it should exhibit, given the previously discussed literature on SMMEs, will be deliberated to offer a detailed understanding. Secondly, the prototype and a detailed discussion of its workings will be introduced. Thirdly, a discussion of the benefits that will accrue from this prototype will follow. Lastly, the results of an evaluation that was performed on the feasibility of the information security governance framework using this prototype will be discussed.

7.2 Desirable Characteristics


Chapter 7 – Information Security Governance Framework Software Prototype & Evaluation
7.1 Introduction
7.2 Desirable Characteristics
7.3 Information Security Governance Framework Software Prototype
7.4 Evaluation of Framework & Software Prototype
7.5 Conclusion

Before the development of the information security governance framework software prototype commenced, the desirable characteristics that it should exhibit were identified and these are detailed below to offer a clear understanding. Hence, based on the previously discussed literature on SMMEs, a series of desirable characteristics will now be highlighted.

SMMEs, by definition, do not typically have the same resources available as their larger counterparts (Koornhof, 2009, p. 83). This is especially true concerning finance, as SMMEs often have an operational budget that is far smaller (Devos et al., 2012; Yildirim et al., 2010). SMMEs therefore require an affordable yet fully operational aid to assist them in their information security governance implementation efforts. Thus, the envisaged prototype should limit the costs involved and the effort that needs to be expended by the enterprise.

SMMEs often have a lack of experience, especially in the area of information security (Goucher, 2011; Upfold & Sewry, 2005). As a result, they often have to rely on expensive security consultants to offer them the experience and guidance they need in this regard (Xiaoping & Jing, 2008). However, these enterprises cannot always afford this expertise and guidance and therefore often resort to cutting corners during their information security governance implementation (Gupta & Hammond, 2005). This may mean that they are extremely vulnerable to information security incidents (Stanley, 2010). SMMEs therefore require a simple do-it-yourself, yet fully operational, aid to assist them in their information security governance implementation efforts. Thus, it is important that the envisaged prototype should require minimal expertise, should be simple to use and understand, and should not rely heavily on overly complex mechanisms.

SMMEs are characterised by their varying size and flexibility in terms of resources and expertise (Koornhof, 2009, pp. 27–28). Often this presents a great difficulty for off-the-shelf information security solutions, as they may not be scalable for usage by such a large variety of business sizes and types (Goucher, 2011). SMMEs therefore require an aid that is scalable and that can adapt to their size, available resources and expertise. Thus, it is vital that the envisaged prototype be highly scalable.

Many off-the-shelf information security solutions are available on the open market. Unfortunately, many of these solutions cater mainly for larger organisations (Barlette & Fomin, 2008). As SMMEs exhibit very distinct features (Koornhof, 2009, pp. 10–28), it is wrong to assume that a single solution will be applicable to both large organisations and smaller enterprises (Sumner, 2009). SMMEs therefore require a tailored aid, which takes into account their unique individualities. Thus, it is essential that the envisaged prototype be tailored specifically for these enterprises and take note of their limitations and restrictions. This requirement is also applicable to the output and input that the prototype offers and requires.

SMMEs are also characterised for their flexibility and adaptive nature (Megginson et al., 2006, p. 9). This includes their size, financial standing and management structures (Devos et al., 2012). However, this often presents great difficulties for these enterprises when they make use of off-the-shelf information security solutions, as some elements may simply not be applicable (Barlette & Fomin, 2008). Thus, it is vital that the envisaged prototype be flexible and allow for a degree of customisation.

Any aid that utilises confidential business information must ensure that the information is securely protected from harm and misuse (ISO/IEC 27002, 2005, p. 83). This is especially true of an aid that uses and stores information pertaining to a SMME’s information security vision and implementation efforts. Thus, it is vital that the envisaged prototype should assure the safety of the enterprise’s personal details as well as the information security data that it will use and store. This may place restrictions on the platform and the mechanisms used for its development.

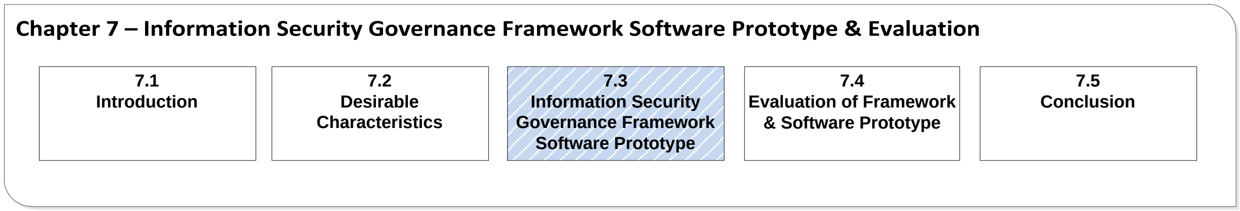
This work has often noted that international information security management and governance standards and best practice, such as ISO/IEC 27002 (2005) and CoBiT 5 (2012a), offer specific guidance that organisations should adhere to if successful information security governance implementation and continued operations are to be ensured. Thus, the envisaged prototype must be based on and adhere to the guidelines offered by international information security management and governance standards and best practices. This will benefit SMMEs as, by using the aid, they will unconsciously also adhere to these guidelines. Furthermore, should the SMME decide to seek an external information security audit, then adherence to such guidelines would be valuable as the necessary measures and documentations would be available to the auditing party.

In summary, the desirable characteristics that should be exhibited by the information security governance framework software prototype, originating from literature of chapters 3, 4 and 5, include:

- affordability
- simplicity
- scalability
- applicability
- flexibility
- safety
- compliance with international information security management and governance standards/best practice.

These principles were subsequently used to develop an information security governance framework software prototype, which will assist SMMEs in their information security governance implementation efforts and challenges. An introduction to this prototype as well as a detailed discussion of its workings follows in the next section.

7.3 Information Security Governance Framework Software Prototype


Chapter 7 – Information Security Governance Framework Software Prototype & Evaluation
7.1 Introduction
7.2 Desirable Characteristics
7.3 Information Security Governance Framework Software Prototype
7.4 Evaluation of Framework & Software Prototype
7.5 Conclusion

A prototype is defined as “an original, full-scale, and usually working model of a new product or new version of an existing product” (*American Heritage Dictionary*, 2011). Prototypes may be constructed to demonstrate that a new model can indeed be implemented and may serve as a vehicle for experimentation (Olivier, 2009, p. 9). Hence, a prototype may be developed to gain more insight into a newly established model or framework.

Of specific interest to this work is a specific type of prototype, namely a proof-of-concept prototype, the major intention of which is to demonstrate that a concept such as a model may work (Olivier, 2009, p. 51). Making use of this type of prototype, the goal is to demonstrate that the main components, relationships and workings of the information security governance framework are in fact implementable. This prototype will subsequently be used to evaluate whether a software package originating from the framework could provide valuable assistance to SMMEs when implementing information security governance.

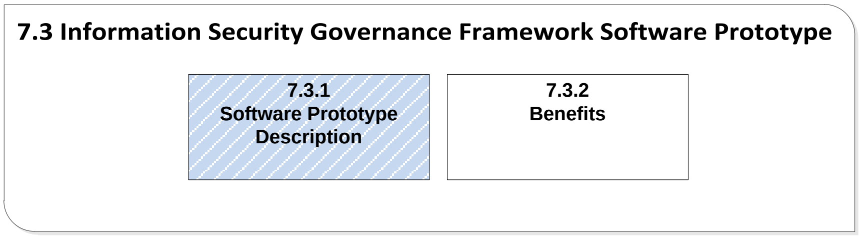
Having defined the purpose and goal of the envisaged prototype, the desirable characteristics (refer to section 7.2, p. 174) were used as guidelines for the development of an proof-of-concept prototype, named *the Information Security Governance Toolbox* (ISGT), which is based on the information security governance framework.

The main components, relationships and workings of this framework (see Figure 6.1, p. 159) were described in the previous chapter (see p. 158–165). These components include the following:

- The execution of the direct–control action cycle
    - including the *direct*, *control* and *execute* actions
- The involvement of various management levels and duties
- The explicit involvement of strategic-level management
- The execution of the *direct* action
    - the development of board directives
    - the establishment of security requirements
    - the development of the information security policy architecture
        - the drafting of the corporate information security policy
        - the drafting of supporting secondary-level policies
        - the drafting of security procedures
        - the selection of security controls
- The execution of the *control* action
    - the execution of a compliance analysis exercise;
    - the aggregation of the compliance analysis exercise results; and
    - the execution of an executive involvement evaluation exercise or similar concept.

A detailed discussion of the way each of these components, relationships and workings were implemented in the proof-of-concept framework prototype follows in the next subsection.

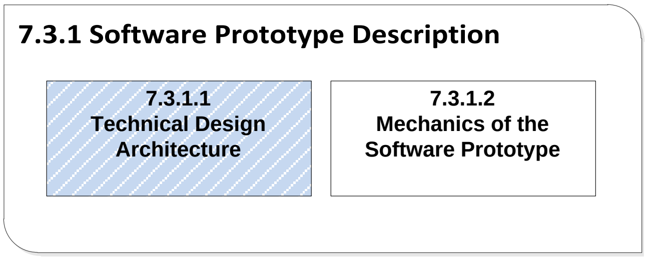
7.3.1 Software Prototype Description


7.3 Information Security Governance Framework Software Prototype
7.3.1
Software Prototype Description
7.3.2
Benefits

The previous chapter described the process leading to the development of an information security governance framework for the implementation of information security governance in organisations. This framework was subsequently used as a basis for the development of a semi-automated proof-of-concept software prototype to guide and assist SMMEs in their information security governance efforts.

As already mentioned, the proof-of-concept software prototype carries the working title of the Information Security Governance Toolbox (ISGT). This prototype extends the functionality offered by an existing information security management prototype software package developed by Hoppe et al. (2002) based on the research conducted by Vermeulen and Von Solms (2002). The extended functionality of the newly developed prototype offers assistance to organisations for the proper implementation of information security governance. This assistance takes the form of establishing board directives, semi-automated drafting of information security policies, security control selection, policy and security control compliance analysis and an executive involvement exercise.

7.3.1.1 Technical Design Architecture


7.3.1 Software Prototype Description
7.3.1.1 Technical Design Architecture
7.3.1.2 Mechanics of the Software Prototype

The Information Security Governance Toolbox (ISGT) was implemented as a stand-alone desktop application using three-tier software architecture in a file-sharing environment. The primary reason for distributing the application's functionally across multiple tiers was to obtain the benefits of a client/server implementation while executing the prototype in a local desktop environment. Having discussed the architectural design considerations, it now becomes necessary to examine the internal workings and components of the software prototype.

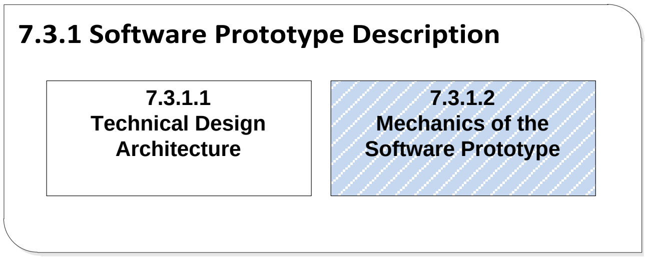
The proof-of-concept software prototype consists primarily of four components. These components map directly onto the requirements embedded in the information security governance framework.

These components of the prototype include:

- an executive directive exercise
- the establishment of information security policy architecture and a security control selection process
- company standards and a security controls compliance analysis exercise
- an executive involvement evaluation exercise.

Furthermore, a knowledge base component was also added to give users of the prototype background information on information security and its proper management and governance. These are the components of the prototype and follow the process flow and usage as determined by the framework.

7.3.1.2 Mechanics of the Software Prototype


7.3.1 Software Prototype Description
7.3.1.1 Technical Design Architecture
7.3.1.2 Mechanics of the Software Prototype

Knowledge Base

> *Objective: To educate the user on the core principles of information security, its management and governance.*

The prototype operates in terms of an interactive wizard with the purpose of accompanying users step by step throughout the process flow specified in the framework. The wizard starts by introducing the user to the knowledge base component. As previously mentioned, this component is responsible for educating the user on the core concepts and principles of information security, its management and governance, as well as emphasising the importance of adhering to a structured and disciplined process when implementing it in an organisation. This module was implemented using a series of pre-established MS PowerPoint slide shows which are embedded in the prototype. Although these slide shows are embedded, they are free-standing in nature and could be frequently updated independently from the prototype to offer the user the latest facts on information security, its management and governance.

User Details Capturing

> *Objective: To facilitate the capturing of the user's organisational information for use during the dynamic drafting of information security documentation by the prototype.*

Once the user has been made aware of the contents of the knowledge base, the next step is for the user to enter his/her personal and/or company details in the fields provided. These may include the company name, company logo, company telephone number, company email address, chief executive officer (CEO) and name of the party responsible for information security. The information captured by these fields is used by the prototype to personalise the documentation that will later be generated as output.

Subsequently, the wizard offers the user an option to follow either the *direct* or the *control phase*. The primary objective of the wizard's *direct phase* is, among other things, to facilitate the establishment of board directives, propose a set of modifiable security controls and semi-automatically draft corresponding information security policies. By contrast, the *control phase* allows the user to perform a compliance analysis exercise in respect of the security controls and company standards established during *the direct phase*, as well as to conduct an executive involvement evaluation exercise in order to evaluate executive management's information security governance involvement and efforts.

The Direct Phase

> *Objective: To facilitate the establishment of board directives, propose a set of modifiable security controls and dynamically draft corresponding information security policies among others.*

Executive Directive Exercise

> *Objective: To assist executive management in the establishment of sound information security board directives by indicating their involvement, commitment and strategic vision for information security.*

The *direct phase* starts with an executive directive exercise. The aim of this exercise is to assist executive management in the establishment of sound information security board directives. Executive management is accordingly asked a series of eleven thought-provoking security-related questions (refer to Addendum D, p. 231). These questions were adapted from the research conducted by R. Von Solms and Von Solms (2006b), as the emanating due care checklist questions offered ease of use and understanding. Further, as the original research assists executive management in establishing a due care and due diligence indicator for its information security governance efforts, it also supports the requirements of the *control phase*. It should, however, be noted that other sets of questions were also identified and considered, but did not afford the same benefits and functionality.

Each of the questions from the research by R. Von Solms and Von Solms (2006b) was adapted to facilitate either a positive (yes) or negative (no) response. In the event of a negative response being submitted, a pre-set information security governance awareness statement and question follows in order to afford executive management an opportunity to re-evaluate and possibly change its initial response. In the event that the initial negative response remains, the wizard then indicates that executive management should seek guidance and education on the matter of information security and its proper governance and will not allow the respondent to progress further. In contrast, as soon as all of the questions have been answered with a positive response, the prototype uses reasoning and inference to establish a corresponding board directive. Thus, if the executive directive exercise is successfully completed (submitted eleven positive responses), a total of eleven corresponding board directives are established (refer to Addendum E, p. 233).

It is worth mentioning that during the development of this component, the above-mentioned and two other approaches were effectively investigated and considered, namely:

- The first approach was to provide executive management with example board directives and to have management draft its own or make use of CoBiT 5's business goals on an IT goals matrix (ISACA, 2012a, fig. 22). Unfortunately this approach required extensive expertise and knowledge on the subject matter, was quite complex and was deemed unfeasible for use by multiple organisations.
- The second approach included simply offering a static list of board directives. Although the easiest and simplest solution, it offered very little flexibility and did not engage executive management sufficiently.
- The third option as per the question list and inference approach, as mentioned above, was deemed the most feasible approach as it requires minimal expertise and knowledge and is not overly complex; thus it is ideal for use by SMMEs.

Information Security Policy Architecture Establishment

> *Objective: To facilitate the establishment of an information security policy architecture in the user organisation by means of security requirement identification, security control proposal and selection and dynamic policy drafting.*

Security requirements analysis

> *Objective: To assist strategic- and tactical-level management with the establishment of security requirements in the user organisation.*

The next step of the *direct phase* entails the establishment of an information security policy architecture. This process consists of a number of steps, the first of which involves the identification of an organisation's security requirements. It was determined that security requirements of an organisation may be formulated by making use of a pre-established business analysis questionnaire consisting of 64 questions based on the security requirements analysis approach, as established by Gerber and Von Solms

(2001). Each of the questions included in the business analysis questionnaire refers to a specific security requirement, namely, confidentiality, integrity, availability, authentication and auditability. However, in order to assess the importance of security requirements properly, each security requirement is addressed by a number of questions in the questionnaire. The answer selected for each of these questions in turn determines a rating (for example; low, medium or high), which is assigned to each security requirement.

It should be noted that during the development of this component, the possibility of performing a traditional risk analysis exercise (refer to subsection 2.3.3.3, p. 48) was also investigated. However, this approach was shown to require extensive knowledge of an organisation's information and IT assets, and the specific threats and vulnerabilities that threaten them, which can vary considerably from organisation to organisation. Further, such a risk analysis involves a great deal of expertise, effort and time, which most SMMEs simply do not have (Barlette & Fomin, 2008). Hence, it was deemed unfit for use in the prototype. Instead, the security requirements analysis approach (Gerber & Von Solms, 2001) was followed, as mentioned above, since it is simpler and allows for greater flexibility and scalability. In retrospect, however, it should be stated that an organisation could still supplement the approach used in the prototype with a risk analysis exercise or other approach, if necessary.

Security control selection

> *Objective: To propose and facilitate the selection of a set of modifiable security controls for the user organisation based on the security requirements established.*

Based upon the identified security requirements and their ratings, the wizard subsequently presents the user with a series of modifiable security controls. These security controls originate from ISO/IEC 27002 (2005) and indicate an appropriate baseline protection for the organisation in line with their security requirements. It should, however, be noted that the security controls presented merely serve as a guide for implementing information security in accordance to the organisation's operational environment. Thus, the user can select or de-select security controls, provided that a legitimate reason is provided in accordance to the statement of applicability proposed by ISO/IEC 27001 (2005, p. 8).

Security control compliance target setting

> *Objective: To allow the user to indicate the desired compliance or adherence level that is sought for each security control selected.*

Concurrent with security control selection, the user is also prompted to indicate the desired compliance or adherence level that is sought for each security control. This constitutes compliance target setting (set at a certain percentage level) for each control. In this regard, the level of compliance ranges from 0 to 100%. The ideal would be to enforce 100%, but since some enterprises using the prototype are only starting to initiate their information security governance implementation, it may be ill-advised to expect such a high compliance level. The desired compliance or adherence level for each security control is in turn stored by the prototype for use during the *control phase*.

Security procedure selection

> *Objective: To propose and facilitate the selection of a set of security procedures for the user organisation based on the security controls selected.*

Subsequent to the completion of the security control selection step, the user is presented with a series of security procedures for each of the security controls. The set of selectable security procedures originates from a variety of sources, of which the implementation guidance clauses of ISO/IEC 27002 (2005) are the primary contributor. This step, that is, the selection of security procedures, is deemed necessary as these serve as a guideline for achieving the objectives of each security control (Bacik, 2008, p. 54; S. Von Solms & Von Solms, 2008, pp. 87–88). It should be noted that currently only security procedures pre-established during the prototype's development can be selected; however, it is envisaged that users may in future add customised security procedures according to their needs or circumstances.

Dynamic generation of information security documentation

> *Objective: To facilitate the dynamic drafting of the security documentation required to enforce the information security measures of the user organisation.*

Following the establishment of the security requirements of the organisation and the selection of appropriate security controls and supportive security procedures, the prototype dynamically drafts the security documentation required to enforce these information security measures.

This documentation includes the drafting of the following:

- a corporate information security policy, both a short and long version (see Addendum A, p. 222)
- secondary-level policies in the form of various supportive company standards that reflect the identified security controls (see Addendum B, p. 228)
- corresponding, policy-linked, security procedures (see Addendum C, p. 230)
- a statement of applicability (see Addendum F, p. 234).

This set of documentation is offered to the user as personalised tailor-made Word documents, which may be modified and adjusted to suit the specific needs of the organisation. The prototype also stores a copy of this documentation, which may be accessed at any time unless new documentation is later drafted.

S. Von Solms and Von Solms (2008, pp. 74–75) indicate that the information security policy architecture of an organisation (see Figure 4.1, p. 111), comprises the components, or documents, that facilitate the directing of information security. Thus, through the dynamic generation by the prototype of this documentation, the information security policy architecture (refer to subsection 4.2.2, p. 110) of the user organisation is established as well as the appropriate selection of information security controls.

The aforementioned components in their entirety constitute the *direct phase* of the prototype, and may be performed whenever the operational environment of the user organisation changes, including when new information and IT assets are purchased or new threats and/or vulnerabilities are identified. It may also be necessary to repeat this phase periodically to ensure that the documentation that has been generated is kept up to date.

The Control Phase

> *Objective: To afford the user a compliance analysis exercise in respect of the security controls and company standards established during the direct phase, as well as to conduct a further executive involvement evaluation exercise to evaluate executive management's information security governance involvement and efforts.*

In support of the framework's requirements and the prototype's *direct phase*, the *control phase* should ideally be initiated at a later date. Owing to the dynamic nature of compliance and adherence, it is advised that this phase should be performed quarterly, bi-annually or at least annually (Posthumus et al., 2010; S. Von Solms & Von Solms, 2008, p. 93). This is because the documentation produced during the *direct phase* does not automatically guarantee compliance and adherence (R. Von Solms & Von Solms, 2006a). Hence, the primary goal of the *control phase* is to evaluate compliance with the documentation produced and then institute corrective action if required.

Company Standards and Security Control Compliance Analysis

> *Objective: To allow the user to perform a compliance analysis exercise in respect of the security controls and company standards established during the direct phase.*

The commencement of the control phase is marked by a company standards and security controls compliance analysis exercise. This exercise starts with the user choosing to perform either a full or limited-scope audit on the established security controls and company standards. In the event that a limited scope is selected, the user is given the option to select the company standards and accompanying security controls that need to be audited. This step allows for flexibility, as an organisation may choose to audit only specific security controls or company standards at a given time to reduce costs and interruptions.

Once a full or limited scope compliance analysis has been selected and an indication provided of the security controls and company standards to be audited, the user is presented with a questionnaire, which contains a series of security control-related audit questions (see Addendum G, p. 238), with at least three questions for each security control selected. A three question minima was opted for to allow for triangulation to occur and a more accurate compliance assessment to be made, especially since SMMEs are often not knowledgeable about security controls and guessing might occur otherwise. Further, three questions is also believed to lead to ease of use and better understandability for SMMEs.

As the security controls that can be selected during the *direct phase* originate from ISO/IEC 27002 (2005), ISO/IEC 27001 (2005) audit questions made available by the InfoSec Institute (2012) were selected for this purpose. Although other sets of questions exist, this set was chosen as it is one of the few that offer more than one audit question per security control. This was deemed vital in making the audit process understandable and for ease of use.

Each of the questions in this set are presented in the form of a five-point Likert scale, on which users indicate the level of security control compliance or adherence achieved, ranging from no adherence or implementation to complete fulfilment and adherence.

When the responses to these questions have been submitted, a graphical audit report (refer to Addendum H, p. 239) is produced using a series of complex mathematical equations and weighted calculations. This report is specifically aimed at tactical- and strategic-level management and makes use of colour coding and key performance indicators (KPIs) to offer a clear indication of the compliance level being achieved for the selected security controls, the company standards and the corporate information security policy as a whole. It is worth mentioning that this report also makes use of the security control compliance target indicators that would have been captured during the security control selection process, to indicate whether the desired outcome has been met.

It is envisaged that this report may in future also be used to indicate compliance with the organisation's security requirements and the board directives established during the *direct phase*, although this has not been done in this prototype.

Due Care Analysis

> *Objective: To facilitate executive management in conducting an executive involvement evaluation exercise to evaluate its information security governance involvement and efforts.*

On completion of the compliance analysis exercise, the next step is to give executive management an opportunity to perform a due care analysis exercise. A series of thought-provoking questions (refer to Addendum I, p. 241) are hereby posed that allow executive management to investigate and evaluate their information security governance efforts in terms of the due care and due diligence required by the framework.

Each question that executive management is asked elicits a positive (yes) or negative (no) response. In turn, the responses indicate executive management's efforts as regards the due care checklist that was developed by R. Von Solms and Von Solms (2006b), which was also used to construct the executive directive exercise component found in the direct phase. Thus, a clear correlation exists between the board directives established by the aforementioned component and the documentation that is generated and the checklist used in this exercise. For example a board directive reads "A Corporate Information Security Policy (CISP) must be defined, introduced and maintained to guide all efforts to mitigate risks threatening business information." Using the prototype a CISP is generated and maintained satisfying the board directive; furthermore this in turn satisfies the due care analysis question "Did you create and express a clear vision to mitigate business information risks to an acceptable level using a CISP".

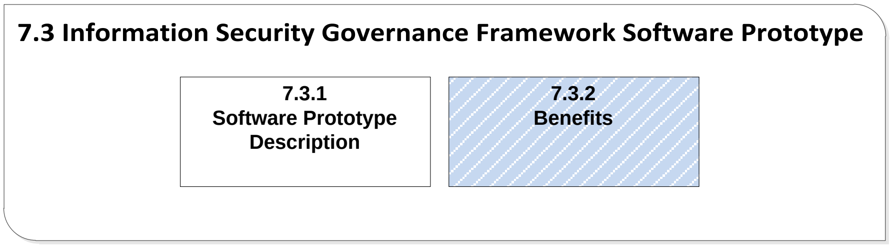
The outcome of this due care analysis exercise, as per R. Von Solms and Von Solms (2006b), provides executive management with a due care and due diligence indicator. Such an indicator may point to a possible lack of due care, which can subsequently assist management in taking corrective action.

These components in their entirety constitute the *control phase* of the prototype. This phase may be performed on a periodic basis as required by the organisation. The *direct* and *control phases* which constitute the workings of this prototype thus combine to form the direct–control action cycle that is exhibited by information security governance (R. Von Solms & Von Solms, 2006a). A series of screenshots illustrating the prototype components and processes can be viewed in Addendum J (p. 242).

The prototype therefore acts as an aid for organisations, in particular SMMEs, when implementing or improving information security governance. This is achieved by the prototype, as it provides actionable components and processes to guide organisations through the information security governance implementation and/or improvement process. The prototype includes the development of relevant information security documentation as well as the maintenance and auditing of such documentation.

As SMMEs are often neither duly aware nor knowledgeable about the above-mentioned components and processes (Koornhof, 2009, pp. 82–83; Yildirim et al., 2010), this prototype offers significant benefits when addressing and possibly alleviating this problem. The following subsection details some of the benefits that may be associated with this prototype.

7.3.2 Benefits

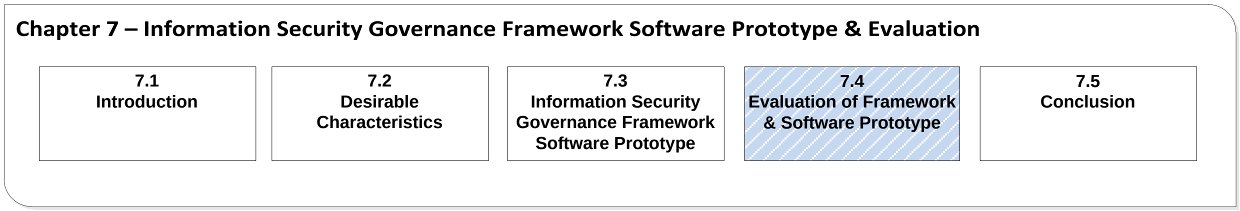

7.3 Information Security Governance Framework Software Prototype
7.3.1
Software Prototype
Description
7.3.2
Benefits

The development of this prototype holds many benefits for SMMEs with limited expertise and resources. This subsection highlights some of the benefits that this prototype provides in relation to the desirable characteristics previously established.

- *Affordability.* By using freely accessible technologies and components for the construction and operation of this prototype, it exhibits the benefit of affordability while also being comprehensive in nature.
- *Simplicity.* During the construction of this prototype, components and techniques were identified and subsequently implemented that are not overly complex and that can be used and interpreted easily. This refers specifically to the security requirements analysis and executive directive exercise. Hence, this prototype exhibits the benefit of simplicity.
- *Scalability.* It was previously indicated that SMMEs are characterised by their varying size and flexibility in terms of resources and expertise (Koornhof, 2009, pp. 82–83; Yildirim et al., 2010). With this in mind, all the techniques and components introduced into this prototype are scalable. Hence, the output of the prototype may be adapted according to the specifics of the organisation using it. Thus, this prototype exhibits the benefit of scalability.
- *Applicability.* Many off-the-shelf information security solutions are available on the open market, but the cater mainly for large organisations (Barlette & Fomin, 2008). This prototype is tailored specifically for SMMEs and takes note of their limitations and restrictions. This also applies to the output and input that this prototype offers and requires. Hence, this prototype exhibits the benefit of applicability.
- *Flexibility.* SMMEs are characterised for their flexibility and adaptive nature (Megginson et al., 2006, p. 9). This includes their size, financial standing and management structures (Devos et al., 2012). As this prototype allows for flexibility and a degree of customisation, it does not limit or restrict the user organisation from using only specific security controls or documentation and so on. Thus, this prototype exhibits the benefit of flexibility.

- *Safety.* An aid that makes use of confidential business information must ensure that information is protected from any harm and misuse (ISO/IEC 27002, 2005, p. 83). This is especially true of an aid that uses and stores information about a SMME's information security implementation and efforts. This prototype ensures the safety of an enterprise's personal details as well as the information security data that it uses and stores, since it was developed as a stand-alone desktop application that requires no network connectivity and uses a password-protected database. Further, all documentation generated by this prototype is stored for safekeeping and may be accessed at any time should the original documentation be damaged or lost. Hence, this prototype exhibits the benefit of safety.
- *Compliance with international information security management and governance standards/best practice.* International information security management and governance standards and best practice offer specific guidance to organisations in order for successful information security governance implementation and continued operations to be assured. This prototype is based on and adheres to the guidance offered by ISO/IEC 27001 (2005), ISO/IEC 27002 (2005) as well as ISO/IEC 38500 (2008) and CoBiT 5 (ISACA, 2012a). Hence, this prototype exhibits the benefit of international information security management and governance standards and best practices compliance.

7.4 Evaluation of Framework and Software Prototype



Chapter 7 – Information Security Governance Framework Software Prototype & Evaluation

7.1
Introduction

7.2
Desirable Characteristics

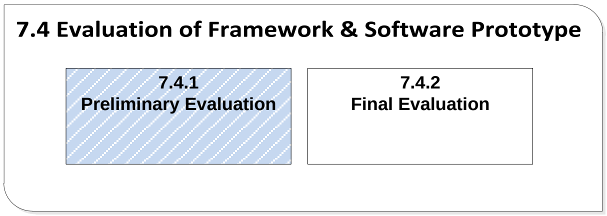
7.3
Information Security Governance Framework Software Prototype

7.4
Evaluation of Framework & Software Prototype

7.5
Conclusion

Having established this proof-of-concept software prototype, it was tested to evaluate the finer workings and components of the framework embedded in it. The evaluation of the framework took place, firstly, whilst constructing the prototype and, secondly, on the basis of feedback received from a focus-group study that was conducted in industry.

7.4.1 Preliminary Evaluation



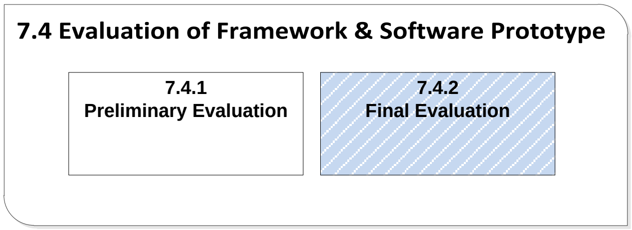
Before the final evaluation of the framework and prototype commenced, a preliminary assessment was performed to gauge whether the prototype was operational and free of errors. This evaluation formed part of the prototype development activities.

The preliminary evaluation was conducted by consulting 60 undergraduate students at a South African university, all of whom are familiar with the field of information security. The main aim of this study was to determine whether the prototype would be feasible and understandable for the intended users. They were requested to report any errors experienced while utilising the prototype, provide feedback on the user interface design and state whether they believed that the prototype added value to the information security community and possibly SMMEs. A questionnaire with both open and closed-ended questions was used to capture the participants' feedback.

Multiple errors and recommendations were captured, subsequently corrected and improvements made prior to the final evaluation. The evaluation results pointed to a consensus that the prototype added value to the information security community and could prove to be highly beneficial to SMMEs. Further, the understandability and user interface design of the prototype were shown to be adequate.

Subsequent to the preliminary evaluation and the above-mentioned corrections being made to the prototype, a final evaluation was performed. The particulars of this follow in the next subsection.

7.4.2 Final Evaluation



Following the completion of the preliminary evaluation of the proof-of-concept software prototype, a focus-group study was conducted to assess the feasibility and benefits of the framework through the use of this prototype.

The framework concepts and prototype were presented and demonstrated at an IT and security conference. On invitation, three respected SMMEs were identified to participate in the focus-group study.

Each participant was visited and underwent a short informative workshop session conducted by the author and developer at their premises, in order to provide them with details on the purpose of the study, an overview of the research and the use of the prototype. Afterwards, this prototype was made available to each of them on a trial-period basis and a questionnaire (see Addendum K, p. 246) was provided, which was to be completed in a specified time in order to evaluate the feasibility of the components and workings of the prototype and, indirectly, the framework.

The research findings that emanated from the responses to this questionnaire (see Addendum L, p. 251) indicated that the applicability, impact, cost-effectiveness and suitability of the prototype and, indirectly, the framework are more than adequate for use by most SMMEs.

Although, the responses suggest that some usability issues still persist in the implementation of the prototype, these have very little effect on its overall application. As this study focused primarily on the conceptualisation of the framework and supporting software prototype, these usability issues are deemed to fall outside the scope of concern. However, these issues will have to be addressed if the decision is made to release a commercial product to industry in the future.

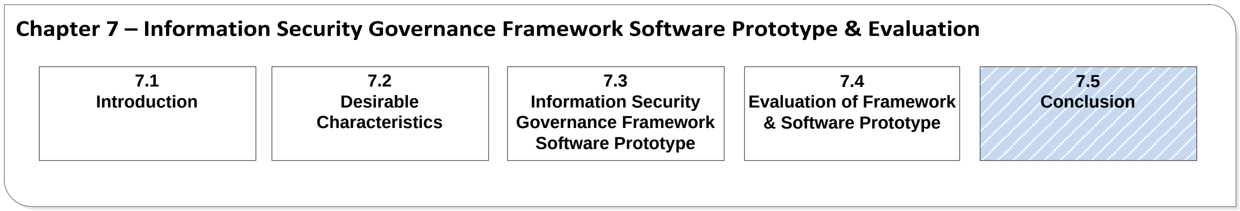
One comment made by a participant in response to an item on the questionnaire indicated that the documentation generated by the prototype and, indirectly, the framework may be too extensive for use by micro or very small enterprises, as it may result in certain maintenance burdens. This comment is acknowledged; however, it should be kept in mind that the prototype is not size-orientated, but rather security requirements-orientated. Accordingly, the security requirements of each individual SMME will directly influence the amount and coverage of the documentation generated by the software prototype and framework.

Another questionnaire respondent raised a concern relating to the fact that certain regulatory issues are not adequately addressed or catered for by the framework, and the software prototype, for example the Protection of Personal Information Bill (POPI). This concern has merit as these regulatory issues are becoming more prominent in industry. In response it can be said that the framework and the software prototype do cater for some regulatory elements to be addressed as part of the security requirements analysis component. However this can certainly be enhanced in future by means of intensive research in this field.

Another respondent made the suggestion that the software prototype should preferably be web-based and make use of a Software-as-a-Service (SaaS) model. This suggestion has been noted and corresponds with the initial vision for the operation and development of the software prototype (Coertze et al., 2011). Unfortunately, given that the software prototype stores and utilises confidential business information, this particular approach was deemed unfeasible for the operation and development of the prototype. Hence, the three-tier desktop application architecture model was adopted instead.

It can thus be concluded from the responses to the questionnaire that the information security governance framework, and the supporting proof-of-concept software prototype, are indeed feasible and hold many benefits for SMMEs in terms of assisting them with their information security governance implementation. Given the suggestions, comments and concerns shared by the questionnaire respondents, the existing prototype and framework may in future be further enhanced to provide even more effective support for SMMEs.

7.5 Conclusion


Chapter 7 – Information Security Governance Framework Software Prototype & Evaluation
7.1 Introduction
7.2 Desirable Characteristics
7.3 Information Security Governance Framework Software Prototype
7.4 Evaluation of Framework & Software Prototype
7.5 Conclusion

This chapter, following the establishment of the information security governance framework, aimed to introduce the reader to a supportive proof-of-concept software prototype that was developed in an attempt to demonstrate the feasibility of the framework. It was indicated that this prototype was specifically intended to assist SMMEs with their information security governance implementation.

This chapter introduced the reader to the desirable characteristics that this prototype needed to exhibit in order to be adopted successfully. These were made apparent by the SMME literature that was discussed previously in this work. In summary these characteristics include:

- affordability
- simplicity
- scalability
- applicability
- flexibility
- safety
- *compliance with international information security management and governance standards/best practice*.

Subsequently, the prototype was introduced in conjunction with a detailed discussion of its components and finer workings. Further, specific mention was made of how the desirable characteristics were addressed in the prototype.

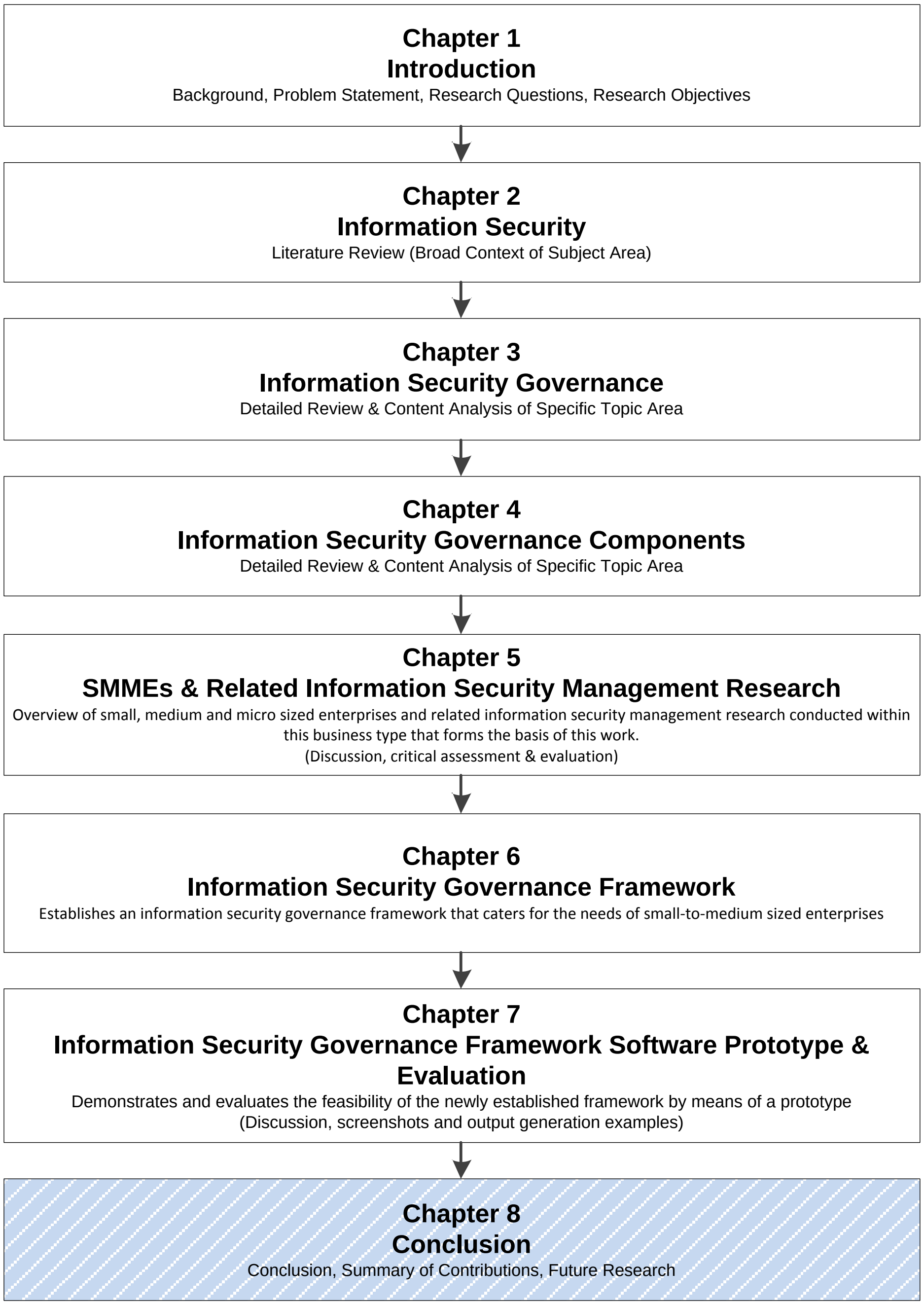
Afterwards, the benefits exhibited by this prototype were highlighted. These benefits were specified as having originated from the information security governance framework upon which it was based, as well as the approaches and techniques that were used for its realisation. These benefits corresponded completely with the desirable characteristics that were deemed necessary prior to its construction.

Having developed the prototype, the framework's finer workings and embedded components were evaluated. This evaluation took the form of a preliminary evaluation that was performed during the prototype's construction and, on completion, a focus-group study that was conducted in industry. The findings of this study suggest that the information security governance framework, and supporting proof-of-concept software prototype, are feasible and hold many benefits when aiding SMMEs with their information security governance implementation. Thus, the framework and supporting software prototype satisfy the objectives and goals that this work initially aimed to achieve.

The following chapter concludes this work by summarising the main findings and contributions made, while also indicating some limitations and future research opportunities. Furthermore, research publications emanating from this work will be mentioned.

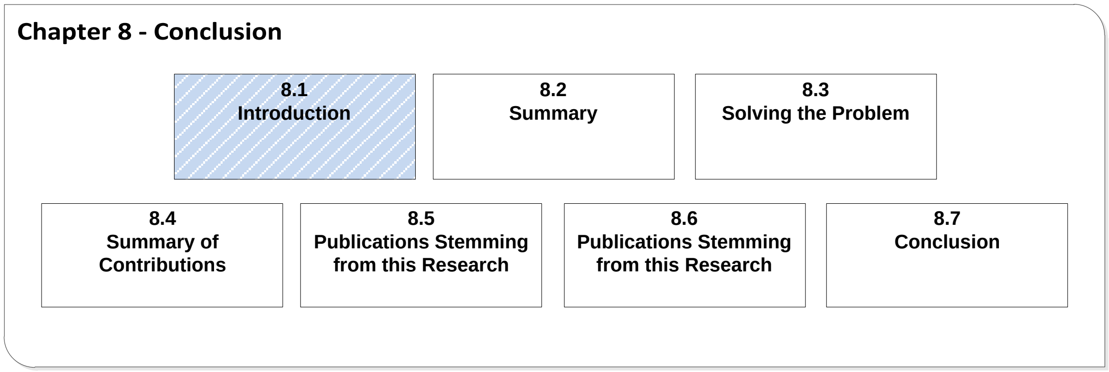
Chapter 8: Conclusion

This chapter aims to conclude this work by summarising the main findings and the contributions it makes, while also indicating some limitations and future research opportunities. Furthermore, research publications emanating from this work will be mentioned.


Chapter 1
Introduction
Background, Problem Statement, Research Questions, Research Objectives
Chapter 2
Information Security
Literature Review (Broad Context of Subject Area)
Chapter 3
Information Security Governance
Detailed Review & Content Analysis of Specific Topic Area
Chapter 4
Information Security Governance Components
Detailed Review & Content Analysis of Specific Topic Area
Chapter 5
SMMEs & Related Information Security Management Research
Overview of small, medium and micro sized enterprises and related information security management research conducted within this business type that forms the basis of this work.
(Discussion, critical assessment & evaluation)
Chapter 6
Information Security Governance Framework
Establishes an information security governance framework that caters for the needs of small-to-medium sized enterprises
Chapter 7
Information Security Governance Framework Software Prototype & Evaluation
Demonstrates and evaluates the feasibility of the newly established framework by means of a prototype
(Discussion, screenshots and output generation examples)
Chapter 8
Conclusion
Conclusion, Summary of Contributions, Future Research

"I think and think for months and years. Ninety-nine times, the conclusion is false. The hundredth time I am right" – Albert Einstein (BrainyQuote, 2012b).

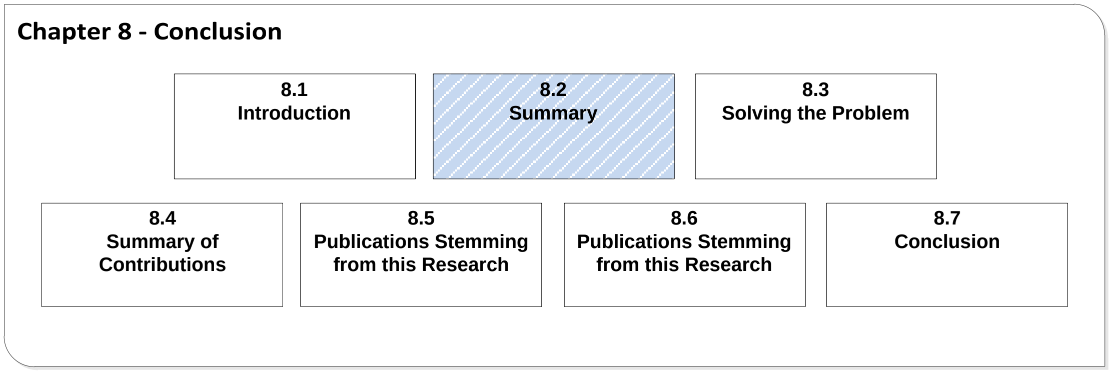
8.1 Introduction


Chapter 8 - Conclusion
8.1 Introduction
8.2 Summary
8.3 Solving the Problem
8.4 Summary of Contributions
8.5 Publications Stemming from this Research
8.6 Publications Stemming from this Research
8.7 Conclusion

The previous two chapters have described the establishment of an information security governance framework and a supportive proof-of-concept software prototype. This chapter concludes the dissertation by summarising the work that has been done and describing how the research objectives set out in the first chapter have been accomplished. Further, the contributions made and further research opportunities presented by this dissertation will be discussed.

The following section presents a summarised account of each chapter and helps to motivate the main argument of this study.

8.2 Summary


Chapter 8 - Conclusion
8.1 Introduction
8.2 Summary
8.3 Solving the Problem
8.4 Summary of Contributions
8.5 Publications Stemming from this Research
8.6 Publications Stemming from this Research
8.7 Conclusion

Chapter 1 introduced the concept of information security and its governance in the context of SMMEs. It highlighted the various problems that had to be considered. It was noted that these enterprises often view information security from a technical standpoint, where by contrast it has to be addressed as a governance issue. Research was subsequently presented that indicates that although some of these enterprises have changed their view in this regard, many still experience grave difficulty in addressing and implementing such governance adequately because of limited expertise and resources. These arguments formed the basis on which this work was conducted. These arguments supported the main objective of this work, which was to develop an information security governance framework supported by a fully functional software prototype in order to assist in governing information security with minimal effort and expertise in the SMME business sector. The research design of the study was also discussed, as following the design science paradigm and related methodology established by Peffers et al. (2007). This methodology included the identification and motivation of a business problem; the establishment of the objectives of a solution; the design and development of the solution, and hence, the framework; the demonstration of the feasibility of the solution by means of a supportive software prototype; the evaluation of the solution, including the framework and prototype, and the communication of the research findings.

Chapter 2 offered further details on information security. The importance of information for the success of modern businesses and IT as an enabler was discussed. Subsequently, it was highlighted that if information is such a vital component and the IT that drives it is so critical, both must be adequately protected. The protection of information was subsequently introduced and evidence was shown that this has existed as a requirement since before the invention of the modern computer. Information protection, known as information security, defends information against unauthorised disclosure, transfer, modification or destruction, whether accidental or intentional. It was emphasised that multiple best practices and standards exist to assist organisations in managing information security. It was further underlined that information, while being transferred, stored and processed using IT, faces many risks. These risks were shown to have a dire impact on organisations if not addressed properly. Consequently, it was argued that a structured process, known as risk management, should be established to mitigate these risks.

Risk management entails identifying the risks pertaining to information assets, identifying possible security controls and then applying them to mitigate the risks identified. Three main categories of security controls were shown to exist, namely, physical, logical and administrative controls. Subsequently, it was highlighted that the first two of these categories depend heavily on the third category in order to be effective. The importance of checking compliance and performing regular audits, which will ensure continued development and improvement of information security, was further emphasised. The chapter concluded with the realisation that information security has changed over the years and that the pervasiveness of information has led to the awareness that executive management has a responsibility towards the proper management and governance of information security. It was revealed that if this is not realised, it may have potentially crippling results for an organisation.

Chapter 3 discussed information security governance in order to understand what would be required from the solution obtained by this work, namely an information security governance framework. It was highlighted that information security governance is an integral part of corporate governance. It was further indicated that information security and IT governance are closely related as both influence information and its protection. These two subject areas, corporate and IT governance were thus described to ensure a better understanding.

It was subsequently demonstrated that everyone in an organisation should be involved in information security, but that executive management remains ultimately accountable. Finally, the requirement for information security governance in all organisations, irrespective of their size, was emphasised. Further, several components, including board directives, policies and compliance monitoring, which may be used to assist in the successful implementation and maintenance of information security governance was mentioned, as the aim of this work was to establish a framework for information security governance.

Chapter 4 introduced and discussed the components that constitute information security governance to offer evidence as to why these components should exist, their purpose and how they may aid in the information security governance process. However, literature was highlighted that suggests that SMMEs are struggling to implement these components and subsequently are having difficulties with their information security governance implementation. This was emphasised as being especially concerning as these enterprises form a significant part of any country's economy and are starting to rely more heavily on information and IT. Consequently, it was argued that a resolution to this problem should be sought.

Chapter 5 introduced the reader to the target audience, SMMEs, of the solution of this work, namely the information security governance framework. It was indicated that SMMEs form a large and important part of economies around the world and are essential in terms of their innovation and flexibility. Further, it was mentioned that IT is now being widely introduced to these enterprises in order to afford them continued growth and competitiveness. Unfortunately, as the dependence on information and its supporting technologies increase, the importance of information protection should also follow. Regrettably, it was shown that these enterprises often experience significant challenges in addressing such protection and therefore often have little or no security measures put in place, especially true of information security governance. Consequently, it was argued that these enterprises require significant assistance in this regard.

Subsequently, the reader was introduced to research relating to this work, which attempts to aid enterprises with managing information security properly. The related research referred primarily to an information security management framework. It was, however, indicated that the vast change in the dependency on IT witnessed globally as well as the need for proper information security governance have resulted in some shortcomings being identified in it. Consequently, it was argued that a revised information security governance framework should be developed.

Chapter 6 established the solution that this work identified, that is, an information security governance framework. This chapter firstly introduced the reader to the principles of the framework, which became evident from the literature discussed. Subsequently, the framework was introduced together with a detailed discussion of its components and finer workings. Further, specific mention was made of the way in which the principles were addressed by the framework. Afterwards, the benefits proffered by this framework were highlighted. These benefits were specified as having originated from the enhancements that were made to the existing information security management framework as well as the realisation of the principles.

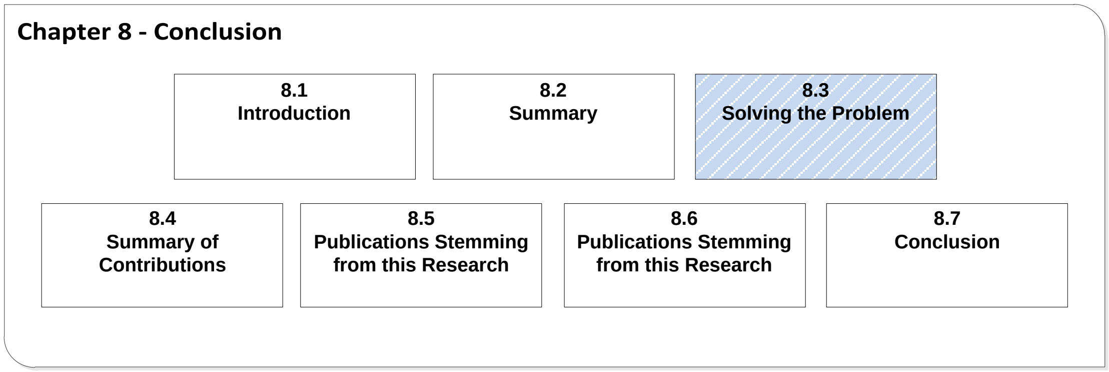
Furthermore, as some organisations have little expertise and experience in implementing information security governance, it is maintained that the level of detail in the proposed framework offers clarity on the tools that can be used and the deliverables that can be expected at each organisational management level. It was, however, emphasised that many other benefits might accrue from the implementation or use of this framework to develop an automated or semi-automated software application targeting information security governance implementation in SMMEs.

Chapter 7 introduced the reader to the supportive proof-of-concept software prototype that was developed in an attempt to demonstrate the feasibility of the framework. This prototype is intended to assist SMMEs in implementing information security governance. This chapter firstly introduced the reader to the desirable characteristics this prototype should demonstrate in order to be adopted successfully. These characteristics were identified in the literature on SMMEs that was discussed. Subsequently, the prototype was introduced together with a detailed discussion of its components and finer workings. Furthermore, specific mention was made of the way these characteristics were addressed in the prototype. Afterwards, the benefits that this prototype exhibits were highlighted. These benefits originated from the information security governance framework upon which the prototype was based as well as the approaches and techniques used to develop it. These benefits corresponded exactly with the desirable characteristics identified.

Having developed the prototype, the finer workings and embedded components of the framework were subsequently evaluated. This took on the form of a preliminary evaluation, which was performed during the construction of the prototype, as well as a focus-group study that was conducted in industry on completion of the prototype. The findings of this suggest that the information security governance framework, and the supporting proof-of-concept software prototype, are feasible and hold many benefits for SMMEs in terms of information security governance implementation. Thus, the framework and the supporting software prototype satisfy the objectives and goals that this work set out to achieve.

These chapters of this study helped to support the main argument. It is, however, important to understand how a solution to this argument was accomplished and how the primary research problem was resolved.

8.3 Solving the Problem


Chapter 8 - Conclusion
8.1 Introduction
8.2 Summary
8.3 Solving the Problem
8.4 Summary of Contributions
8.5 Publications Stemming from this Research
8.6 Publications Stemming from this Research
8.7 Conclusion

The primary research problem for this dissertation was stated as (see p. 21):

> Many SMMEs do not comply with sound information security governance principles, specifically those of information security policy drafting and compliance monitoring; this is mainly as a result of limited resources and expertise.

This problem statement helped define the primary objective of the study which was (see p. 22):

> to develop a framework, supported by a fully functional software prototype, to assist in governing information security with minimal effort and expertise in the SMME sector.

A number of secondary objectives were defined to help accomplish the primary objective of the study and provide a resolution to the problem statement (see p. 22).

The first of these secondary objectives was *"to determine the current state of information security governance in SMMEs"*. This dissertation achieved this secondary objective by introducing, firstly, information security governance and, secondly, literature on these enterprises. Specific mention was made of their unique characteristics, their importance to the world economy and their current challenges. Further, literature was highlighted that offers comprehensive evidence that information security and its governance remains a significant challenge for these enterprises and that they are in dire need of assistance in this regard.

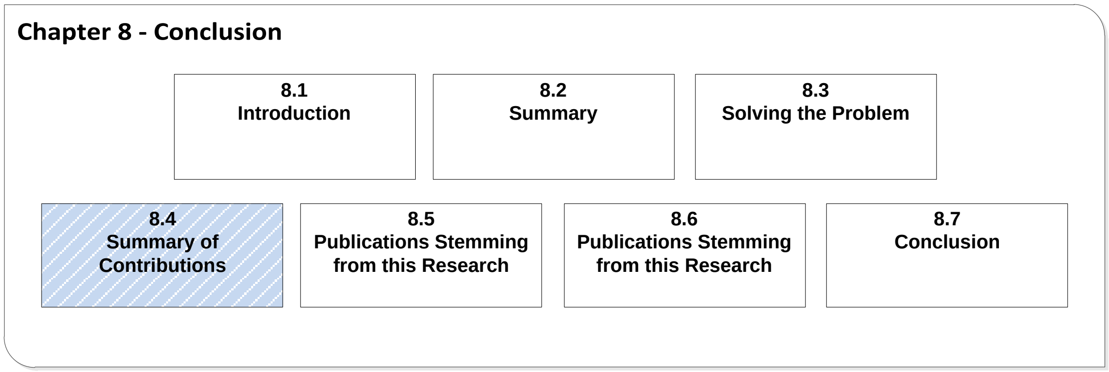
The second of these secondary objectives was *"to determine the principles that must be exhibited by a framework to assist in the sound implementation of information security governance by SMMEs"*. This objective was accomplished by integrating and contextualising the literature related to information security governance and SMMEs. The components and actions that constitute information security governance were identified and the unique characteristics of SMMEs investigated. Given this information, a series of principles was determined, which governed the development of the solution of this work.

The third secondary objective was *"to develop an information security governance framework for implementing proper information security governance in an organisation"*. This objective was accomplished through the establishment of an information security governance framework targeting the implementation and improvement of information security governance in SMMEs. This framework depicted the components and actions that should be implemented and monitored by SMMEs in order to address information security and its continued management and governance successfully.

The fourth secondary objective was *"to validate the framework by using a software prototype implementation to assist SMMEs in their information security governance implementation"*. This objective was accomplished by the development of a proof-of-concept software prototype, namely the Information Security Governance Toolbox (ISGT), which was subsequently used to validate the framework on which it was originally based.

Thus, by meeting these four secondary objectives of the dissertation, the primary objective, *"to develop a framework, supported by a fully functional software prototype, to assist in governing information security with minimal effort and expertise in the SMME sector"*, was achieved.

8.4 Summary of Contributions

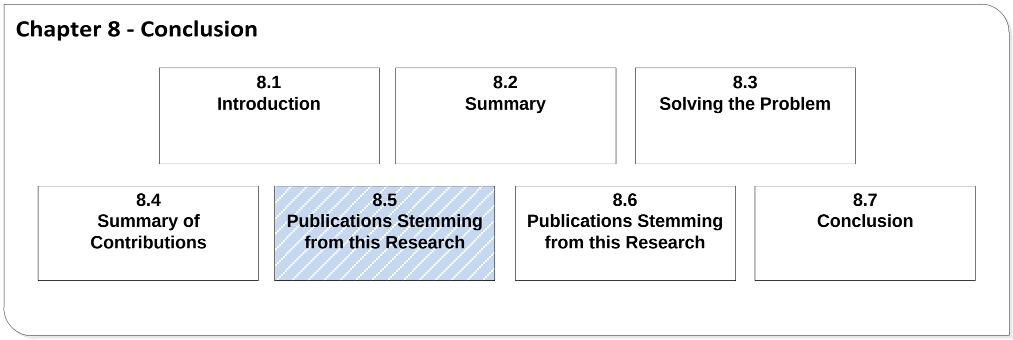

Chapter 8 - Conclusion
8.1 Introduction
8.2 Summary
8.3 Solving the Problem
8.4 Summary of Contributions
8.5 Publications Stemming from this Research
8.6 Publications Stemming from this Research
8.7 Conclusion

The work in this dissertation led to three primary contributions. These are summarised briefly here:

- Firstly, an information security governance framework has been established (see Figure 6.1, p. 159) that expands on the direct–control action cycle established by R. Von Solms and Von Solms (2006a; 2008, pp. 3–4). This framework makes a significant contribution to the body of work on this topic, as it offers further details on the specifics that constitute information security governance, especially the *direct* and *control* actions. Moreover, it addresses and resolves the inadequacies identified in previous information security management research conducted by Vermeulen and Von Solms (2002). Additionally, with the establishment of this framework, the development of future information security governance software packages, for the support of different sized organisations, will now be developed and implemented with more ease.

- Secondly, this framework has introduced a new concept in the form of an executive directive exercise (see subsection 7.3.1.2, p. 182). This exercise adds a significant contribution to the work on this topic, as the literature review identified that it is the first of its kind. This could in future be expanded and possibly used in areas other than information security governance in order to assist executive management in establishing a clear vision and strategy. This could apply particularly to IT and corporate governance.
- Finally, the development of a proof-of-concept software prototype makes a significant contribution to this body of work, as it demonstrates that the framework that was developed is feasible and has the capability of assisting SMMEs in their information security governance implementation. Although these enterprises were the target audience of this work, the prototype may also be used and expanded to address larger organisations in future. Further, this prototype could also be used as the basis for developing future information security governance software packages or products.

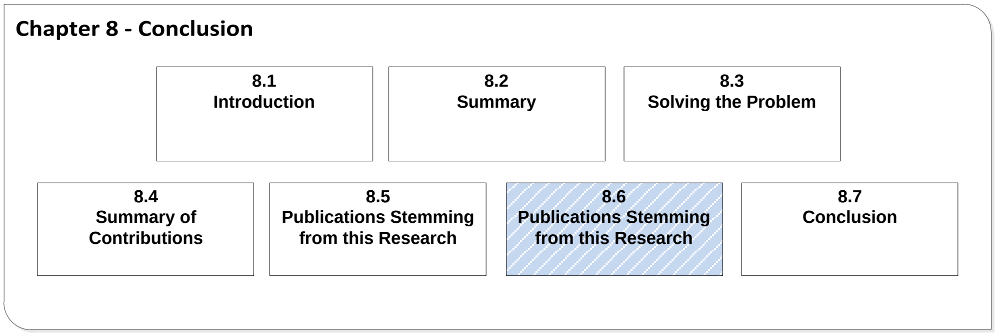
8.5 Publications Stemming from this Research


Chapter 8 - Conclusion
8.1 Introduction
8.2 Summary
8.3 Solving the Problem
8.4 Summary of Contributions
8.5 Publications Stemming from this Research
8.6 Publications Stemming from this Research
8.7 Conclusion

The following publications have resulted directly from the work in this dissertation:

- Coertze, J., & Von Solms, R. (2012). A model for information security governance in developing countries. *AfriComm* (pp. 1–8). Springer. [Best Paper]
- Coertze, J., Van Niekerk, J., & Von Solms, R. (2011). A web-based Information Security Management Toolbox for small-to-medium enterprises in southern Africa. *Information Security South Africa (ISSA)* (pp. 1–8). IEEE. doi:10.1109/ISSA.2011.6027515

8.6 Suggestions for Further Research


Chapter 8 - Conclusion
8.1 Introduction
8.2 Summary
8.3 Solving the Problem
8.4 Summary of Contributions
8.5 Publications Stemming from this Research
8.6 Publications Stemming from this Research
8.7 Conclusion

As the evaluation of the information security governance framework, by means of the prototype, took place primarily in South Africa, future research could be conducted to evaluate its impact and effectiveness in other countries, as it may be especially useful in resource-scarce developing African countries, among others.

As the target audience for this work was SMMEs, research could be conducted to expand this framework and the prototype for use by larger organisations. Although many off-the-shelf information security governance solutions exist to assist such organisations, a simplified yet comprehensive solution may prove to be more financially and operationally beneficial.

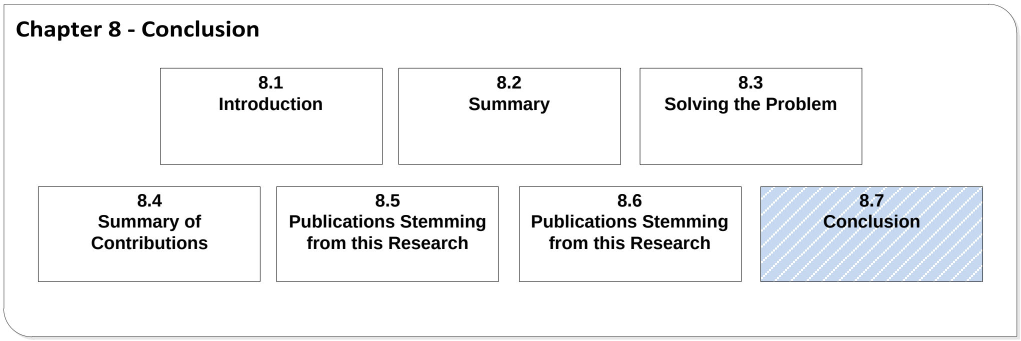
As the executive directive exercise embedded in the framework is believed to be the first of its kind, research may be required to escalate its comprehensiveness and to evaluate its impact and effectiveness. This is also true of the question and inference approached used within this exercise in this work. Further, as indicated above, this exercise may be adjusted to support other areas where executive management is required to establish a vision and strategy as well. The author suggests that this may be especially helpful in the areas of corporate and IT governance.

During the research and the development of the framework and prototype, no reference could be found to a single set of security procedures that is directly mapped to the security controls of ISO/IEC 27002 (2005). Thus, research may be conducted to establish such a comprehensive set of mapped security procedures. Accordingly, this might prove to be highly beneficial for future information security implementations.

Although it was originally envisaged that the security control audit questionnaire would include questions related to security procedures, this proved to be too difficult. Hence, research could be conducted to establish an audit questionnaire for operational staff or management to evaluate their adherence to and application of security procedures in terms of security controls.

A major difficulty experienced with auditing security control implementation and adherence is that the audit questions are generally directed at the organisation's technical staff who would have implemented the controls from the outset; hence an objective assessment can seldom be made. Research should therefore be conducted to design an audit questionnaire for operational staff in order to enhance the evaluation of compliance with and adherence to security control levels more comprehensively in the organisation. Given the responses of both the technical and operational staff, such an questionnaire would prove highly beneficial in obtaining a more objective view of security control compliance.

8.7 Conclusion


Chapter 8 - Conclusion
8.1 Introduction
8.2 Summary
8.3 Solving the Problem
8.4 Summary of Contributions
8.5 Publications Stemming from this Research
8.6 Publications Stemming from this Research
8.7 Conclusion

Information security is an extremely stimulating and ever-changing field. This is especially true because the information security community has transitioned from a management to a governance perspective.

However, ensuring proper information security governance remains a daunting task for many organisations, as those businesses without the resources and expertise needed to implement information security and ensure its proper governance find themselves at risk of security breaches and incidents. Hence, any assistance that could provide these organisations with an affordable and simple yet comprehensive information security governance solution could prove to be highly beneficial.

This dissertation offered such assistance in the form of a proof-of-concept software prototype, based on the information security governance framework developed in this work. This framework and the supportive prototype exhibit properties that make the solution affordable, scalable, flexible and simplistic and, thus, ideal for use by SMMEs.

Bibliography

Abraham, S. E. (2012). IT, an enabler in corporate governance. *Corporate Governance*. doi:10.1108/14720701211234555

Abu-Musa, A. (2010). Information security governance in Saudi organizations: an empirical study. *Information Management & Computer Security*, *18*(4), 226–276. doi:10.1108/09685221011079180

Andreassen, T. (2011). *The Practice of Corporate Social Responsibility among Small, Micro and Medium Manufacturing Enterprises in the Pietermaritzburg Area and how this Practice is Influenced by their Stakeholders*. University of KwaZulu-Natal.

Andress, J. (2011). *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice*. (R. Rogers, Ed.). Elsevier.

Ashenden, D. (2008). Information Security management: A human challenge? *Information Security Technical Report*, *13*(4), 195–201. doi:10.1016/j.istr.2008.10.006

Bacik, S. (2008). *Building an Effective Information Security Policy Architecture* (pp. 1–360). CRC Press.

Barlette, Y., & Fomin, V. V. (2008). Exploring the Suitability of IS Security Management Standards for SMEs. *Proceedings of the 41st Annual Hawaii International Conference on System Sciences (HICSS 2008)*, 308–308. doi:10.1109/HICSS.2008.167

Baskerville, R., Dhillon, G., & Stahl, B. C. (2011). Creativity and Intelligence in Small and Medium Sized Enterprises: The Role of Information Systems. *IFIP Advances in Information and Communication Technology*, 1–9.

Beachboard, J., Cole, A., Mellor, M., Hernandez, S., & Aytes, K. (2008). Improving Information Security Risk Analysis Practices for Small- and Medium-Sized Enterprises: A Research Agenda. *Issues in Information Science and Information Technology*, *5*.

Beaver, G., & Prince, C. (2004). Management, strategy and policy in the UK small business sector: a critical review. *Journal of Small Business and Enterprise Development*, *11*(1), 34–49. doi:10.1108/14626000410519083

Beranek, L. (2011). Risk analysis methodology used by several small and medium enterprises in the Czech Republic. *Information Management & Computer Security*, *19*(1), 42–52. doi:10.1108/09685221111115854

Bhattacharya, D. (2008). *Leadership Styles and Information Security in Small Businesses: An Empirical Investigation*. University of Phoenix.

Boubala, H. (2010). *Risk management of SMMEs*. Cape Peninsula University of Technology.

Bougaardt, G., & Kyobe, M. (2011). Investigating the Factors Inhibiting SMEs From Recognizing and Measuring Losses From Cyber Crime in South Africa. *Electronic Journal Information Systems Evaluation*, *14*(2), 167–178.

BrainyQuote. (2012a). Marshall McLuhan Quotes. Retrieved November 8, 2012, from http://www.brainyquote.com/quotes/quotes/m/marshallmc386841.html

BrainyQuote. (2012b). Albert Einstein Quotes. Retrieved November 9, 2012, from http://www.brainyquote.com/quotes/quotes/a/alberteins109019.html

Brotby, K. (2006). *Information Security Governance: Guidance for Boards of Directors and Executive Management* (2nd ed.). IT Governance Institute.

Brotby, K. (2008). *Information Security Governance: Guidance for Information Security Managers*. IT Governance Institute.

Brotby, K. (2009). *Information Security Governance: A Practical Development and Implementation Approach*. Honoken, New Jersey: John Wiley & Sons.

Burns, A., Davies, A., & Davies, P. (2006). A study of the uptake of Information Security Policies by small and medium sized businesses in Wales. *Small*, *10*(49).

Business Roundtable. (2010). *Principles of Corporate Governance*. Retrieved from http://businessroundtable.org/uploads/studies-reports/downloads/2010_Principles_of_Corporate_Governance_1.pdf

BusinessDictionary.com. (2012). Standard. Retrieved August 22, 2012, from http://www.businessdictionary.com/definition/standard.html

Butler, R., & Butler, M. (2010). Beyond King III: Assigning accountability for IT governance in South African enterprises. *South African Journal of Business Management*, *41*(March), 33–45.

Chalaris, I., & Lemos, P. P. (2005). IT Governance: The Safe Way to Effective and Efficient Governance. *E-Journal of Science and Technology*, *1*(1), 59–63. doi:10.1.1.130.6135

Chipperfield, C., & Furnell, S. (2010). From security policy to practice: Sending the right messages. *Computer Fraud & Security*, *2010*(3), 13–19. doi:10.1016/S1361-3723(10)70025-7

Chiware, E. R. T., & Dick, A. L. (2008). Information Needs and Information Seeking Patterns of Small, Medium and Micro Enterprises in Namibia. *Information Development*, *24*(1), 24–36. doi:10.1177/0266666907087694

Clinch, J. (2009). ITIL V3 and Information Security. *Best Management Practice: For Portfolio, Programme, Project, Risk and Service Management*, (May), 1–40.

Coertze, J., Van Niekerk, J., & Von Solms, R. (2011). A web-based Information Security Management Toolbox for small-to-medium enterprises in Southern Africa. In *Information Security for South Africa* (pp. 1–8). IEEE. doi:10.1109/ISSA.2011.6027515

Coleman, T., & Chatfield, A. (2011). Promises And Successful Practice In IT Governance: A Survey Of Australian Senior IT Managers. In *Pacific Asia Conference on Information Systems (PACIS)*.

David, J. (2002). Policy enforcement in the workplace. *Computers & Security*, *21*(6), 506–513. doi:10.1016/S0167-4048(02)01006-4

De Haes, S., & Van Grembergen, W. (2008). Analysing the Relationship Between IT Governance and Business/IT Alignment Maturity. *Proceedings of the 41st Annual Hawaii International Conference on System Sciences (HICSS 2008)*, 428–428.

Devos, J., Landeghem, H., & Deschoolmeester, D. (2012). Rethinking IT governance for SMEs. *Industrial Management & Data Systems*, *112*(2), 206–223. doi:10.1108/02635571211204263

Dictionary.com. (2012). Negligence. Retrieved August 22, 2012, from http://dictionary.reference.com/browse/negligence?s=t

Dlamini, M., Eloff, J., & Eloff, M. (2009). Information security: The moving target. *Computers & Security*, *28*(3-4), 189–198. doi:10.1016/j.cose.2008.11.007

Dojkovski, S., Lichtenstein, S., & Matthew, W. (2007). Fostering information security culture in small and medium size enterprises: an interpretive study in Australia. In *ECIS* (pp. 1560–1571).

Drucker, P. (1993). *Management challenges for the 21st Century*. Harpers Business.

Du Plessis, J., Hargovan, A., & Bagaric, M. (2011). *Principles of Contemporary Corporate Governance* (2nd ed.). New York, USA: Cambridge University Press.

Editors of the American Heritage Dictionaries. (2011). *The American Heritage Dictionary of the English Language*. *The American Heritage Dictionary of the English Language* (5th ed., p. 2112). Houghton Mifflin Harcourt.

Ernst & Young. (2009). *Outpacing change: Ernst & Young's 12th annual global information security survey*. Retrieved from http://www.b3b.ch/wp-content/uploads/12th_annual_GISS.pdf

EU Recommendation 361. (2003). *Official Journal of the European Union*, 36–41.

Forbes.com. (2012). Thoughts from Philip S. Delaney. Retrieved November 8, 2012, from http://thoughts.forbes.com/thoughts/philip-s-delaney

Futcher, L. (2011). *An Integrated Risk-Based Approach to Support IT Undergraduate Students in Secure Software Development*. Nelson Mandela Metropolitan University.

Gerber, M., & Von Solms, R. (2001). From Risk Analysis to Security Requirements. *Computers & Security*, *20*(7), 577–584. doi:10.1016/S0167-4048(01)00706-4

Gerber, M., & Von Solms, R. (2005). Management of risk in the information age. *Computers & Security*, *24*(1), 16–30. doi:10.1016/j.cose.2004.11.002

Gerber, M., & Von Solms, R. (2008). Information security requirements – Interpreting the legal aspects. *Computers & Security*, *27*(5-6), 124–135. doi:10.1016/j.cose.2008.07.009

Gerber, M., Von Solms, R., & Overbeek, P. (2001). Formalizing information security requirements. *Information Management & Computer Security*, *9*(1), 32–37. doi:10.1108/09685220110366768

Goucher, W. (2011). Do SMEs have the right attitude to security? *Computer Fraud & Security*, *2011*(7), 18–20. doi:10.1016/S1361-3723(11)70075-6

Gregory, P. (2003). *Enterprise Information Security - Information security for non-technical decision makers*. Pearson Education.

Grobler, T., & Von Solms, S. (2004). Assessing the Policy Dimension. *Johannesburg, South Africa: Technikon*.

Gupta, A., & Hammond, R. (2005). Information systems security issues and decisions for small businesses: An empirical examination. *Information Management & Computer Security*, *13*(4), 297–310. doi:10.1108/09685220510614425

Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, *47*(2), 154–165. doi:10.1016/j.dss.2009.02.005

Hevner, A., March, S., Park, J., & Ram, S. (2004). Design science in information systems research. *Mis Quarterly*, *28*(1), 75–105.

Hone, K., & Eloff, J. (2009). Information security governance: business requirements and research directions. *Corporate Ownership & Control*, *7*(1).

Hoppe, O. A., Van Niekerk, J., & Von Solms, R. (2002). The Effective Implementation of Information Security in Organizations. In *Proceedings of the IFIP TC11 17th International Conference on Information Security. Visions and Perspectives* (pp. 1–18). Deventer, The Netherlands: Kluwer, B.V.

Horn, A. (n.d.). Information Security - More Than An IT Challenge For SME. Retrieved September 14, 2012, from http://www.freshbusinessthinking.com/business_advice.php?CID=3&AID=2629&PGID=1

Huang, R., Zmud, R., & Price, R. (2009). IT governance practices in small and medium-sized enterprises: recommendations from an empirical study. *Small and Medium-Sized Enterprises*.

Information Security Forum. (2007). *The Standard of Good Practice for Information Security*. *Information Security* (pp. 1–26).

InfoSec Institute. (2012). ISO27002 Security Framework Audit Program Template. Retrieved September 28, 2012, from http://resources.infosecinstitute.com/iso27002-template/

Institute of Directors in Southern Africa. (1994). *King Report on Corporate Governance*.

Institute of Directors in Southern Africa. (2002). *King II Report on Corporate Governance*.

Institute of Directors in Southern Africa. (2009a). *King III Report on Corporate Governance*. Parklands.

Institute of Directors in Southern Africa. (2009b). *King Code of Governance for South Africa*.

ISACA. (2012a). *COBIT 5*.

ISACA. (2012b). *CobiT 5 for Information Security*.

ISO/IEC 27001. (2005). *Information technology: Security techniques - Information security management systems - Requirements*. Switzerland: International Organization for Standardization (ISO).

ISO/IEC 27002. (2005). *Information technology: Code of practice for information security management* (pp. 1–135). Switzerland: International Organization for Standardization (ISO).

ISO/IEC 27005. (2008). *Information technology: Security techniques - Information security risk management*. Switzerland: International Organization for Standardization (ISO).

ISO/IEC 38500. (2008). *Corporate governance of IT*. International Organization for Standardization (ISO).

IT Governance Institute. (2003). *Board Briefing for IT Governance* (2nd ed.). Information Systems Audit and Control Association.

IT Governance Institute. (2007). *Cobit 4.1*. ISACA.

IT Governance Institute. (2008). *Unlocking Value: An Executive Primer on the Critical Role of IT Governance*.

Jansson, K. (2011). *A Model for Cultivating Resistance to Social Engineering Attacks*. Nelson Mandela Metropolitan University.

Kankanhalli, A., Teo, H., Tan, B., & Wei, K. (2003). An integrative study of information systems security effectiveness. *International Journal of Information Management*, *23*(2), 139–154. doi:10.1016/S0268-4012(02)00105-6

Kimwele, M., Mwangi, W., & Kimani, S. (2011). IT Security Framework for Kenyan Small and Medium Enterprises (SMEs). *International Journal of Computer Science and Security*, *5*(1), 39–53.

Knapp, K. J., Franklin Morris Jr., R., Marshall, T. E., & Byrd, T. A. (2009). Information security policy: An organizational-level process model. *Computers & Security*, *28*(7), 493–508. doi:10.1016/j.cose.2009.07.001

Koornhof, H. (2009). *A Framework for IT Governance in Small Businesses*. *Information Security*. Nelson Mandela Metropolitan University.

Krishna, M. (2010). *A Methodology for Measuring Information Security Maturity in Norwegian and Indian MSME's with special focus on people factor*. Gjovik University College.

Lazarides, T., & Drimpetas, E. (2008). The missing link to an effective corporate governance system. *Corporate Governance*, *8*(1), 73–82. doi:10.1108/14720700810853419

Le Roux, F. (2010). *The Applicability of The Third King Report on Corporate Governance to Small and Medium Enterprises*. Stellenbosch University.

Lessing, M., & Von Solms, S. (2008). Building a world class information security governance model. In *IST-Africa* (pp. 1–9).

Levy, M. (2009). *An Exploration of the Role of Information Systems in Developing Strategic Growth in Small and Medium-sized Enterprises*. University of Warwick.

Love, P., Reinhard, J., Schwab, A., & Spafford, G. (2010). *Global Technology Audit Guide (GTAG) 15 Information Security Governance* (pp. 1–28). Altamonte Springs, USA: The Institute of Internal Auditors.

Lubbe, S., & Jokonya, O. (2009). Using information technology governance, risk management and compliance (GRC) as a creator of business values – a case study. *South African Journal of Economic and Management Sciences*, *12*(1), 115–125.

Macaulay, A. (2004). Enterprise architecture design and the integrated architecture framework. *Microsoft Architect Journal*, (January).

March, S., & Smith, G. (1995). Design and natural science research on information technology. *Decision Support Systems*, *15*(4), 251–266. doi:10.1016/0167-9236(94)00041-2

McAfee. (2009). *The Security Paradox*. America: Santa Clara.

Megginson, L., Byrd, M., & Megginson, W. (2006). *Small business management: an entrepreneur's guidebook* (5th ed.). New York, USA: McGraw-Hill/Irwin.

National Archives (Great Britain). (2008). *Managing Information Risk: A Guide for Accounting Officers, Board Members and Senior Information Risk Owners* (pp. 1–44). Retrieved from https://www.nationalarchives.gov.uk/services/publications/information-risk.pdf

Nolan, R., & McFarlan, F. (2005). Information technology and the board of directors. *Harvard Business Review*.

Olivier, M. (2009). *Information Technology Research: A Practical Guide for Computer Science and Informatics* (3rd ed., pp. 1–178). Pretoria, South Africa: Van Schaik.

Organisation for Economic Co-operation and Development. (2004). *OECD Principles of Corporate Governance*.

Oxford Dictionary. (2010). *Oxford Dictionary of English*. *Oxford Dictionary of English* (3rd ed.). Oxford University Press.

O'Brien, E., & Robertson, P. (2009). Future leadership competencies: from foresight to current practice. *Journal of European Industrial Training*, *33*(4), 371–380. doi:10.1108/03090590910959317

Pasic, A., Rodriguez, P., & Torres, J. (2008). Information security governance. In *ICSTISGIG Conference*.

Peffers, K., Tuunanen, T., Gengler, C. E., Rossi, M., Hui, W., Virtanen, V., & Bragge, J. (2006). The design science research process: a model for producing and presenting information systems research. In *Proceedings of the First International Conference on Design Science Research in Information Systems and Technology (DESRIST 2006)* (pp. 83–106).

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A Design Science Research Methodology for Information Systems Research. *Journal of Management Information Systems*, *24*(3), 45–77. doi:10.2753/MIS0742-1222240302

Pfleeger, C., & Pfleeger, S. (2006). *Security in Computing* (4th ed.). Prentice Hall.

Pironti, J. P. (2006). Information security governance: Motivations, benefits and outcomes. *Information Systems Control Journal*, 2–5.

Posthumus, S., Von Solms, R., & King, M. (2010). The board and IT governance : The what, who and how. *South African Journal of Business Management*, *41*(3), 23–32.

President. National Small Business Act (1996). Government Gazette.

President. National Small Business Amendment Act (2003). Government Gazette.

President. National Small Business Amendment Act (2004). Government Gazette.

Queensland Government. (2001). *Best Practice Guide - Information Risk Management*.

Quotes Star. (2012). A pinch of probability is worth a pound of perhaps. Retrieved November 9, 2012, from http://www.quotesstar.com/quotes/a/a-pinch-of-probability-is-113465.html

Rainer, R., & Cegielski, G. (2010). *Introduction to Information Systems: Supporting and Transforming Business* (3rd ed.). Wiley.

Raynard, P., & Forstater, M. (2002). *Corporate Social Responsibility: Implications for Small and Medium Enterprises in Developing Countries*.

Rees, J. (2010). Information security for small and medium-sized business. *Computer Fraud & Security*, *2010*(9), 18–19. doi:10.1016/S1361-3723(10)70123-8

Richardson, R. (2008). CSI computer crime and security survey. *Computer Security Institute*.

Robinson, N. (2007). The Many Faces of IT Governance: Crafting an IT Governance Architecture. *Information Systems Control*, 1–4.

Rogerson, C. (2004). The impact of the South African government's SMME programmes: a ten-year review (1994-2003). *Development Southern Africa*, *21*(5), 765–784. doi:10.1080/0376835042000325697

Smedinghoff, T. (2008). The State of Information Security Law: A Focus on the Key Legal Trends. *EDPACS*, *37*(1-2), 1–52. doi:10.1080/07366980701838449

Smit, Y., & Watkins, J. A. (2012). A literature review of small and medium enterprises (SME) risk management practices in South Africa. *African Journal of Business Management*, *6*(21), 6324–6330. doi:10.5897/AJBM11.2709

Stanley, N. (2010). *The Ongoing Security Paradox*. United Kingdom, London.

Stavroulakis, P., & Stamp, M. (2010). *Handbook of Information and Communication Security*. Berlin, Heidelberg: Springer Berlin Heidelberg. doi:10.1007/978-3-642-04117-4

Sumner, M. (2009). Information Security Threats: A Comparative Analysis of Impact, Probability, and Preparedness. *Information Systems Management*, *26*(1), 2–12. doi:10.1080/10580530802384639

Sánchez, L., Ruiz, C., Fernández-Medina, E., & Piattini, M. (2010). Managing the Asset Risk of SMEs. *2010 International Conference on Availability, Reliability and Security*, *60*, 422–429. doi:10.1109/ARES.2010.52

Tarantino, A. (2008). *Governance, Risk, and Compliance Handbook*. Hoboken, New Jersey: John Wiley & Sons.

Tawileh, A., Hilton, J., & McIntosh, S. (2007). Managing information security in small and medium sized enterprises: a holistic approach. *Proceedings of the ISSE/SECURE*, 331–339.

Upfold, C. T., & Sewry, D. A. (2005). An investigation of Information Security in Small and Medium Enterprises (SMEs) in the Eastern Cape. In H. S. Venter, J. H. P. Eloff, L. Labuschagne, & M. M. Eloff (Eds.), *Proceedings of the ISSA 2005 New Knowledge Today Conference* (pp. 1–17).

Vacca, J. (2009). *Computer and Information Security Handbook*. Elsevier.

Van Bon, J. (2011). *ITIL - A Pocket Guide*.

Van Grembergen, W., & De Haes, S. (2009). *Enterprise Governance of IT*. Boston, MA: Springer US. doi:10.1007/978-0-387-84882-2

Vermeulen, C., & Von Solms, R. (2002). The information security management toolbox - taking the pain out of security management. *Information Management & Computer Security*, *10*(3), 119–125. doi:10.1108/09685220210431872

Von Solms, R. (1998). Information security management (1): why information security is so important. *Information Management & Computer Security*, *6*(4), 174–177. doi:10.1108/EUM0000000004533

Von Solms, R., Thomson, K., & Maninjwa, P. (2011). Information Security Governance control through comprehensive policy architectures. In *2011 Information Security for South Africa* (pp. 1–6). IEEE. doi:10.1109/ISSA.2011.6027522

Von Solms, R., & Von Solms, S. (2004). From policies to culture. *Computers & Security*, *23*(4), 275–279. doi:10.1016/j.cose.2004.01.013

Von Solms, R., & Von Solms, S. (2006a). Information Security Governance: A model based on the Direct–Control Cycle. *Computers & Security*, *25*(6), 408–412. doi:10.1016/j.cose.2006.07.005

Von Solms, R., & Von Solms, S. (2006b). Information security governance: Due care. *Computers & Security*, *25*(7), 494–497. doi:10.1016/j.cose.2006.08.013

Von Solms, S. (2001). Information Security – A Multidimensional Discipline. *Computers & Security*, *20*(6), 504–508. doi:10.1016/S0167-4048(01)00608-3

Von Solms, S. (2006). Information Security – The Fourth Wave. *Computers & Security*, *25*(3), 165–168. doi:10.1016/j.cose.2006.03.004

Von Solms, S., & Von Solms, R. (2008). *Information Security Governance* (pp. 1–134). Springer.

Wall, D. (2005). The internet as a conduit for criminal activity. In A. Patavina (Ed.), *Information Technology and the Criminal Justice System*. Sage Publications.

West, R. (2008). The psychology of security. *Communications of the ACM*, *51*(4).

Whitman, M., & Mattord, H. (2012). *Principles of information security* (4th ed.). Course Technology.

Wong, K. (2005). Critical success factors for implementing knowledge management in small and medium enterprises. *Industrial Management & Data Systems*, *105*(3), 261–279.

Xiaoping, Y., & Jing, F. (2008). Review of IT/IS Adoption and Decision-Making Behavior in Small Businesses. *Tsinghua Science and Technology*, *13*(3), 323–328.

Yildirim, E., Akalp, G., Aytac, S., & Bayram, N. (2010). Factors influencing information security management in small- and medium-sized enterprises: A case study from Turkey. *International Journal of Information Management*. doi:10.1016/j.ijinfomgt.2010.10.006

Addendum A

Corporate Information Security Policy Sample

Preface

Management has realized that information is one of the most important, if not thé most important, asset in our organization. Timely and accurate information is imperative towards the success of our organization. For this reason, management has determined a need for, and is committed to, ensuring proper information security in this organization.

This policy document serves to outline management's expectations of our IT systems and employees as far as securing information are concerned. All information security, any related activities and personnel are required to abide by this policy document. Any deviations to the policies outlined in this document, must first be authorized by senior management or the information security officer.

Our organization must operate and be perceived as a safe and reliable company that ensures the security of the information assets, the reputation of the organization and the staff optimally.

It is the intention of management that these security policies should dictate a new culture in our organization and become a natural part of the daily work of every employee.

____

Chief Executive Officer

1. Objectives

Information is an asset that, like other important business assets, is essential to an organization’s business and consequently needs to be suitably protected. This is especially important in the increasingly interconnected business environment. As a result of this increasing interconnectivity, information is now exposed to a growing number and a wider variety of threats and vulnerabilities.

Information can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by post or by using electronic means, shown on films, or spoken in conversation. Whatever forms the information takes, or means by which it is shared or stored, it should always be appropriately protected.

Information security is the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities.

The objective of this Policy is to define and propagate an environment that will ensure that our company's information assets are properly protected. These information assets includes, data stored electronically, transmitted across networks, transmitted by fax, printed or written on paper, or spoken in conversations, meetings and over the telephone.

This policy aims to uphold the following objectives:

1. Ensure that our company is perceived as a reliable and respected business partner,
2. Ensure correct access to the information of the organization,
3. Limit the impact of any damage to a defined and accepted scope and
4. Protect against violation or attempted violation of the security regulations and measures and ensure that violation or attempted violation can be discovered and tracked to the relevant person(s).

This Policy will be supported by at least the following two documents:

- A Guideline for Information Security Controls, including a set of security controls selected from the ISO/IEC 27002 standard meeting the Information Security Requirements defined by the organization, and
- A Guideline for Information Security Procedures, consisting of a set of rules, regulations and procedures to be followed by users of information.

2. Scope of Influence

The influence of this policy spans the whole organization, including all business areas and all geographically distributed sites.

3. Policy Statements

It is the Policy of our company:

1. Compliance (See Compliance Policy)
   - To avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements.
2. Business Continuity Management (See Business Continuity Management Policy)
   - To counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.
3. Information Systems Acquisition, Development and Maintenance (See Information Systems Acquisition, Development and Maintenance Policy)
   - To prevent errors, loss, unauthorized modification or misuse of information in applications.
   - To reduce risks resulting from exploitation of published technical vulnerabilities.
4. Information Security Incident Management (See Information Security Incident Management Policy)
   - To ensure a consistent and effective approach is applied to the management of information security incidents.

4. Roles and Responsibilities

For this Policy to be effectively implemented, it is essential that security related roles are defined and that specific responsibilities are assigned to each of these roles.

1. **Role:** CEO and Senior Management

   Responsibilities:

   - Formally endorse and actively support this Policy

2. **Role:** Information Security Officer

   Responsibilities:

- To develop, implement and periodically review the information security policy, procedures and controls

3. **Role:** Information Security Forum

Responsibilities:

- Review and approve information security policy
- Monitor significant changes in the exposure of information assets to threats
- Review and monitor security incidents
- Approve major initiatives to enhance information security
- Actively promote information security within the organization

4. **Role:** Information Owners

Responsibilities:

- Authorize access and assign custody of information
- Communicate the control requirements to the custodian and users of the information
- Determine the statutory requirements regarding retention and privacy of the information, and communicate this information to the custodian

5. **Role:** Custodian

Responsibilities:

- Implementation of physical and technical controls
- Identifying procedural guidelines for the users
- Administering access to information
- Evaluate the cost-effectiveness of controls

6. **Role:** Users

Responsibilities:

- Use the information only for the purpose intended by the owner
- Comply with all the controls established by the owner and custodian
- Ensure that classified or sensitive information is not disclosed to anyone without permission from the owner

- Ensure that his/her identification and passwords are not disclosed to or used by others

5. Approach to Risk Management

A comprehensive Information Security Management System will be defined, implemented and maintained, based on our specific information security requirements and ISO/IEC 27002 (a standard based on best practices and inter-organizational trust).

6. Outsourcing Management

An outsourcing contract between parties, addressing the potential risks, security controls and procedures for information systems and/or desk top environments must be in place before the work can commence.

7. Information Security and Awareness

The Information Security Officer is responsible to provide appropriate training to all users of information, including management, on:

- The contents of this policy,
- The specific information security controls and procedures introduced and
- Their responsibility towards the Policy and meeting the information security objectives.

8. Legal and Regulatory Requirements

All statutory, regulatory or contractual security requirements should be explicitly defined and documented for each information system. In addition to this, appropriate procedures should be implemented to ensure legal compliance to:

- Intellectual property rights, e.g. copyright, trademarks, etc.,
- Safeguarding of organizational records,
- Misuse of information processing facilities,
- Regulation of cryptographic controls and
- Collection of evidence.

9. Incident Handling

All information security incidents or suspected/potential security incidents must be reported to the Help Desk or Information Security Officer by email or in any written format.

10. Compliance to Policy

This information security policy will be supported with standards, setting minimum levels for controls and procedures, on how to meet the security requirements identified. These controls and procedures will be reviewed and audited regularly to ensure on-going compliance with the standards set.

11. Penalties and Consequences

In the event of contravening any aspect of this Policy, the organization's normal disciplinary procedures will take effect.

Or

In the event of violating any aspect of this Policy, the following penalties may be incurred:

- Written warning (first offense)
- Revocation of security privileges on the system (second offense)
- Suspension from work (third offense)
- Dismissal from work plus legal action (fourth offense)

12. Maintenance of Policy

The Information Security Officer will be responsible for the maintenance of the Policy on a continual basis or following any major security incident, acquisition or implementation of hardware and/or software, change to the Scope of Influence to this policy or any event affecting the applicability of this Policy.

Addendum B

Company Standard Sample

Information Systems Acquisition, Development and Maintenance Policy

Objective(s):

- To prevent errors, loss, unauthorized modification or misuse of information in applications.
- To reduce risks resulting from exploitation of published technical vulnerabilities.

12.2 Correct Processing in Applications

12.2.1 Input data validation

Data input to applications should be validated to ensure that this data is correct and appropriate.

12.2.2 Control of internal processing

Validation checks should be incorporated into applications to detect any corruption of information through processing errors or deliberate acts.

12.2.3 Message integrity

Requirements for ensuring authenticity and protecting message integrity in applications should be identified, and appropriate controls identified and implemented.

12.2.4 Output data validation

Data output from an application should be validated to ensure that the processing of stored information is correct and appropriate to the circumstances.

12.6 Technical Vulnerability Management

12.6.1 Control of technical vulnerabilities

> Timely information about technical vulnerabilities of information systems being used should be obtained, the organizations exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk.

Additional information concerning the implementation, maintenance and assurance of these security controls can be found in the document: Supporting Procedures of Information Systems Acquisition, Development and Maintenance. (See Addendum C)

Addendum C

Security Procedures Sample

Supporting Procedures of Information Systems Acquisition, Development and Maintenance Policy

Procedure 1: Input Data Validation and Rejected Item Handling (12.2.1)

All transactions to be input to a multi-user computer system must first be subjected to reasonableness checks, edit checks, and/or validation checks. Transactions which fail such checks must either be: (a) rejected with a notification of the rejection sent to the submitter, (b) corrected and resubmitted, or (c) suspended pending further investigation.

Procedure 2: Need for Cross-Validation of Important Information (12.2.2)

Important information on which management depends must be periodically compared with external sources or otherwise cross-validated to ensure that it conveys an accurate representation of reality.

Procedure 3: Originator of Transactions Must Be Clearly Identified (12.2.3)

Transactions affecting sensitive, critical, or valuable information must be initiated only by source documents or computerized messages in which the originating individual or system is clearly identified.

Procedure 4: Plausibility Checks (12.2.4)

Plausibility checks must be performed to test whether the output date is reasonable

Procedure 5: Action Response on Potential Technical Vulnerabilities (12.6.1)

Appropriate, timely action should be taken in response to the identification of potential technical vulnerabilities.

Addendum D

Board Directive Questions Sample Set

1. Information is an important business asset to your organization. Do you agree with this statement?

2. It has been agreed that business information is a valuable asset. Do you agree that a definite effort must be made to determine which are the most critical risks threatening the well-being of these valuable information assets?

3. Business information is important to the organization and that critical risks pose a serious threat to the organization. Do you agree that a Corporate Information Security Policy (CISP) must be created to express a clear vision from executive management to mitigate business risks to an acceptable level?

4. A CISP must be drafted and introduced in the organization. Do you agree that this fairly high-level policy must be technically, operationally and managerially disseminated and expressed as secondary-level policies in the form of company standards and/or issue-specific policies to allow for its adoption by the rest of the organization?

5. Considering that secondary-level policies in the form of company standards will lead to security controls to be implementation within the organization. Do you agree that resources (budget, manpower, technology) must be made available, as far as possible, to successfully implement these controls?

6. Company standards must be enforced in the organization. Do you agree that adequate procedures and guidelines must be put in place to operationally enforce them?

7. An ineffective Corporate Information Security Policy and supporting company standards add little value or protection. Do you agree that these must be assessed and monitored for efficiency?

8. Most information workers are unaware of information security and secure practices. Do you agree that all the information workers in the company must be adequately educated and made aware of information security, acceptable behavioural procedures and guidelines?

9. Considering the frequent change seen in information technology, threats and risks, do you agree that a definite process must be defined to ensure that the policies, company standards, controls and procedures are updated regularly?

10. Considering that security might be faulty or inefficient, do you agree that a process must be put in place to continuously monitor security controls to identify any exceptions or deviations?

11. Some security controls may be inefficient, out-dated or possibly absent. Do you agree that all security related internal controls (including operational controls) must be audited for proper functioning and complete coverage?

Addendum E

Board Directives Sample

1. Information is critical to the well-being of the organization.

2. A structured approach to mitigate all business risks related to organizational information must be defined, implemented and maintained.

3. A Corporate Information Security Policy (CISP) must be defined, introduced and maintained to guide all efforts to mitigate risks threatening business information.

4. The Corporate Information Security Policy must be supported by secondary-level policies to allow for the dissemination of the technical, operational and managerial aspects thereof.

5. All company security standards and related controls must be technical, operational and managerial interpreted and implemented within the organization and resources must be made available to do so.

6. Adequate procedures and guidelines must be defined to operationally enforce company security policies and standards.

7. Timely audits must be performed to determine the effectiveness of the Corporate Information Security Policy, the supporting company standards and controls.

8. All employees must be effectively educated and made aware of security policies, procedures and guidelines.

9. A definite process must be defined and implemented to ensure that the policies, company standards, controls and procedures are updated regularly.

10. A process must be in place to continuously monitor the effectiveness of security controls to identify any exceptions or deviations to enable the duly updating thereof.

11. All security related internal controls (including operational controls) must be audited at regular intervals for proper functioning and complete coverage.

Addendum F

Statement of Applicability Sample

8.2.2 Information security awareness, education, and training

All employees of the organization and, where relevant, contractors and third party users should receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function.

This control was added by default.

12.2.1 Input data validation

Data input to applications should be validated to ensure that this data is correct and appropriate.

This control was added by default.

12.2.2 Control of internal processing

Validation checks should be incorporated into applications to detect any corruption of information through processing errors or deliberate acts.

This control was added by default.

12.2.3 Message integrity

Requirements for ensuring authenticity and protecting message integrity in applications should be identified, and appropriate controls identified and implemented.

This control was added by default.

12.2.4 Output data validation

Data output from an application should be validated to ensure that the processing of stored information is correct and appropriate to the circumstances.

This control was added by default.

12.6.1 Control of technical vulnerabilities

Timely information about technical vulnerabilities of information systems being used should be obtained, the organizations exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk.

This control was added by default.

13.2.1 Responsibilities and procedures

Management responsibilities and procedures should be established to ensure a quick, effective, and orderly response to information security incidents.

This control was added by default.

13.2.2 Learning from information security incidents

There should be mechanisms in place to enable the types, volumes, and costs of information security incidents to be quantified and monitored.

This control was added by default.

13.2.3 Collection of evidence

Where a follow-up action against a person or organization after an information security incident involves legal action (either civil or criminal), evidence should be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).

This control was added by default.

14.1.1 Including information security in the business continuity management process

A managed process should be developed and maintained for business continuity throughout the organization that addresses the information security requirements needed for the organizations business continuity.

This control was added by default.

14.1.2 Business continuity and risk assessment

Events that can cause interruptions to business processes should be identified, along with the probability and impact of such interruptions and their consequences for information security.

This control was added by default.

14.1.3 Developing and implementing continuity plans including information security

Plans should be developed and implemented to maintain or restore operations and ensure availability of information at the required level and in the required time scales following interruption to, or failure of, critical business processes.

This control was added by default.

14.1.4 Business continuity planning framework

A single framework of business continuity plans should be maintained to ensure all plans are consistent, to consistently address information security requirements, and to identify priorities for testing and maintenance.

This control was added by default.

14.1.5 Testing, maintaining and re-assessing business continuity plans

Business continuity plans should be tested and updated regularly to ensure that they are up to date and effective.

This control was added by default.

15.1.2 Intellectual property rights (IPR)

Appropriate procedures should be implemented to ensure compliance with legislative, regulatory, and contractual requirements on the use of material in respect of which there may be intellectual property rights and on the use of proprietary software products.

This control was added by default.

15.1.3 Protection of organizational records

Important records should be protected from loss, destruction, and falsification, in accordance with statutory, regulatory, contractual, and business requirements.

This control was added by default.

15.1.4 Data protection and privacy of personal information

Data protection and privacy should be ensured as required in relevant legislation, regulations, and, if applicable, contractual clauses.

This control was added by default.

Addendum G

Security Control Audit Questionnaire Sample

8. Human Resources Security

8.2. During Employment

8.2.2. Information security awareness, education, and training

1. Do all employees of the organization and, where relevant, contractors and third party users receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function?

1 2 3 4 5

Never/Not Always/Fully

2. Does awareness training commence with a formal induction process designed to introduce the organization's security policies and expectations before access to information or services is granted?

1 2 3 4 5

Never/Not Always/Fully

3. Does on-going training include security requirements, legal responsibilities and business controls, as well as training in the correct use of information processing facilities e.g. log-on procedure, use of software packages and information on the disciplinary process?

1 2 3 4 5

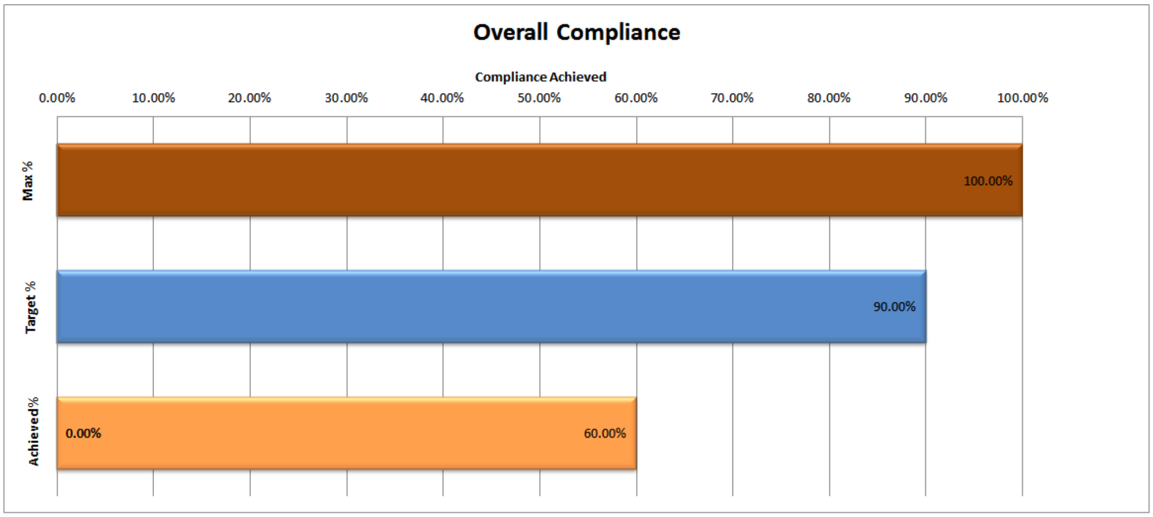
Never/Not Always/Fully

Addendum H

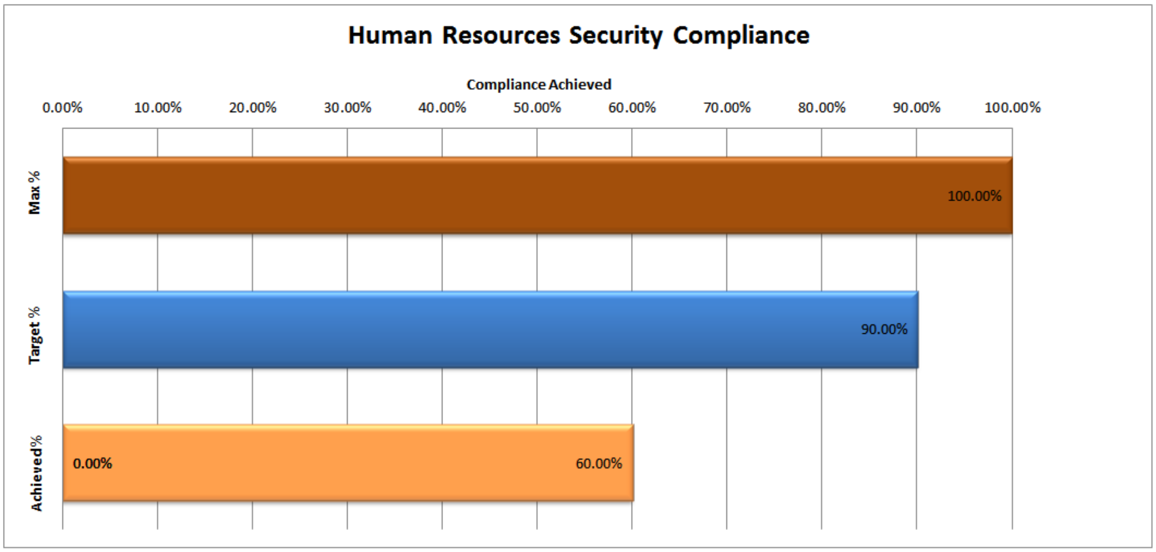
Audit Report Sample

28 September 2012

	Policies	Maximum	Target	Actual	Gap %
7	Asset Management	0	0	0	0.00%
8	Human Resources Security	15	13.5	9	33.33%
9	Physical and Environmental Security	0	0	0	0.00%
10	Communications and Operations Management	0	0	0	0.00%
11	Access Control	0	0	0	0.00%
12	Information Systems Acquisition, Development and Maintenance	0	0	0	0.00%
13	Information Security Incident Management	0	0	0	0.00%
14	Business Continuity Management	0	0	0	0.00%
15	Compliance	0	0	0	0.00%
		15	**13.5**	**9**	**33.33%**



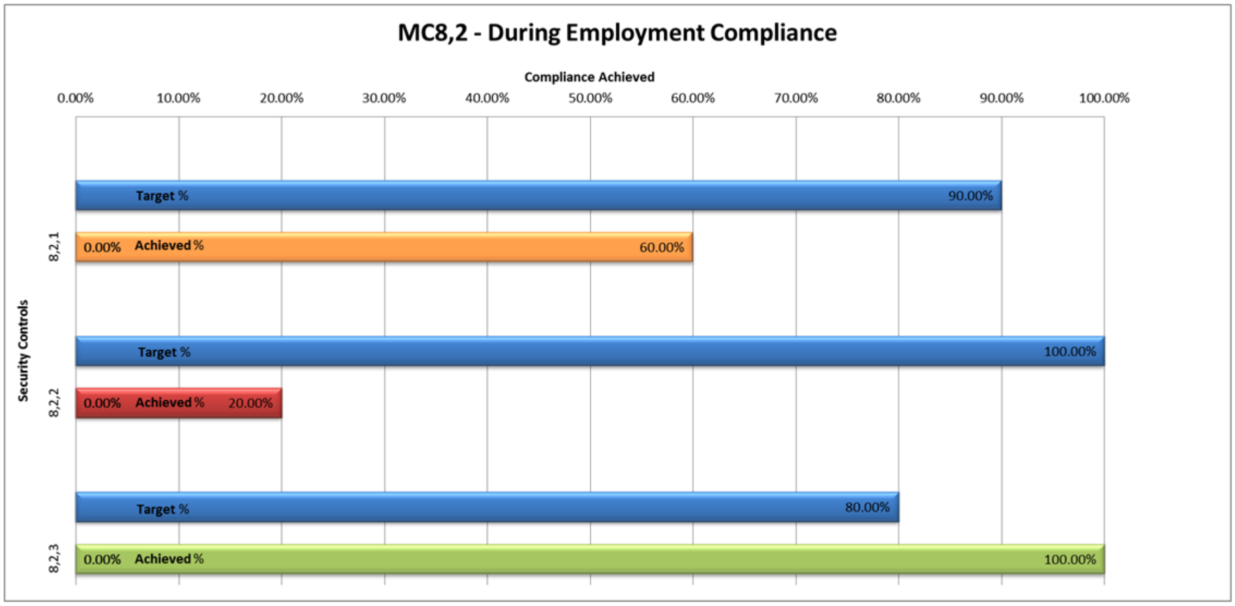
	Security Categories	Maximum	Target	Actual	Gap %
8.1	Prior to Employment	0	0	0	0.00
8.2	During Employment	15	13.5	9	33.33
8.3	Termination or Change of Employment	0	0	0	0.00
		15	**13.5**	**9**	**33.33**



Main Security Category: 8.2 During Employment

	Security Controls	Actual	Max	Max %	Target %	% Achieved
8.2.1	Management responsibilities	3	5	100.00%	90.00%	60.00%
8.2.2	Information security awareness, education, and training	1	5	100.00%	100.00%	20.00%
8.2.3	Disciplinary process	5	5	100.00%	80.00%	100.00%

Maximum:	15
Target:	13.5
Actual:	9
Gap	**4.5**



Addendum I

Due Care Checklist Questions Sample Set

1. Do you accept that information is a critical important business asset to your organisation?

2. Have you made an asserted effort to determine which the most critical risks are threatening the organisation's information assets

3. Did you create and express a clear vision to mitigate these risk to an acceptable level

4. Did you ensure that the corporate information security policy (CISP) was technically, operationally and managerially interpreted to be implemented in a practical manner?

5. Did you ensure that the required resources (budget, manpower, technology) were made available, as far as possible, to implement the company security standards?

6. Are you convinced that adequate procedures and guidelines were put in place to operationally enforce these company security policies and standards?

7. Are you convinced that the CISP and company security standards are effective?

8. Were all information workers in the company adequately educated on acceptable behavioural procedures and guidelines?

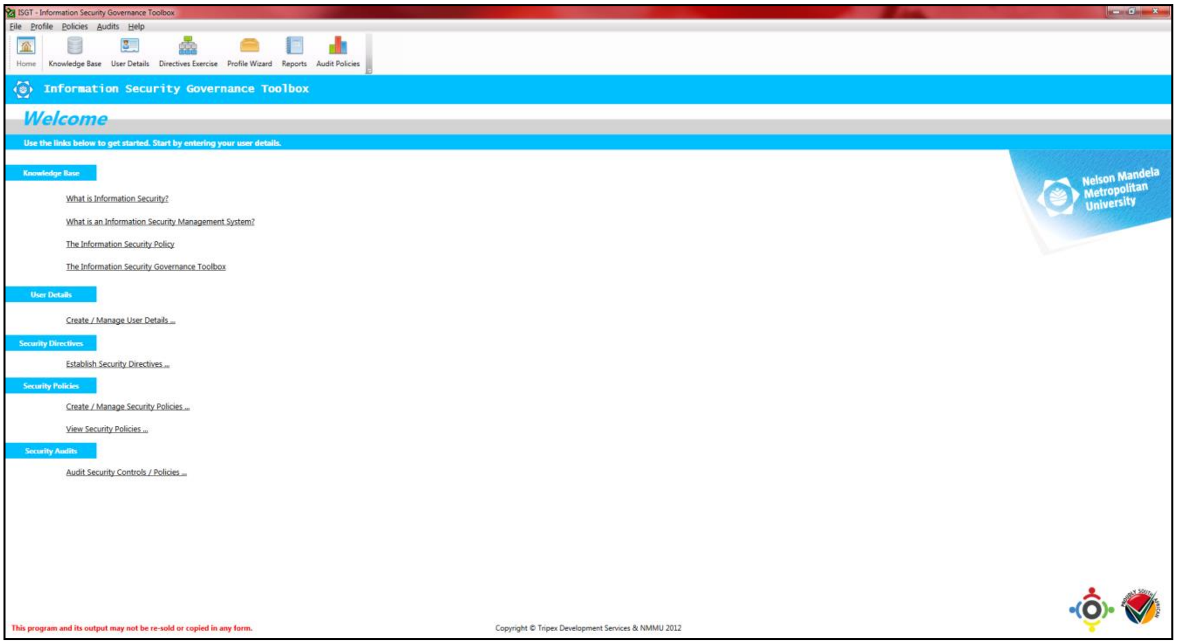
9. Is a definite process in place that ensures that the policies, company standards and procedures are updated with regular intervals?

10. Is a process in place to continuously monitor security controls to identify any exceptions or deviations?

11. Are all security related internal controls (including operational controls) audited for proper functioning?

Addendum J

Information Security Governance Toolbox Screenshots


ISGT - Information Security Governance Toolbox
File Profile Policies Audits Help
Home
Knowledge Base
User Details
Directives Exercise
Profile Wizard
Reports
Audit Policies
Nelson Mandela Metropolitan University

Information Security Governance Toolbox

Welcome

Use the links below to get started. Start by entering your user details.

Knowledge Base

What is Information Security?

What is an Information Security Management System?

The Information Security Policy

The Information Security Governance Toolbox

User Details

Create / Manage User Details ...

Security Directives

Establish Security Directives ...

Security Policies

Create / Manage Security Policies ...

View Security Policies ...

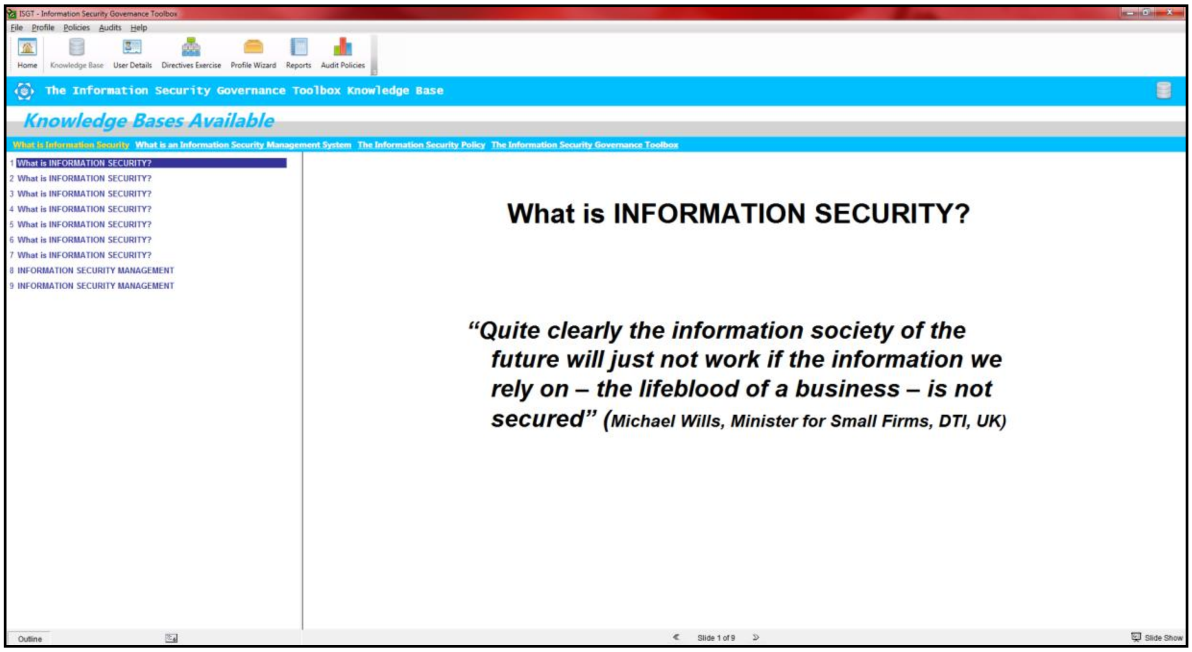
Security Audits

Audit Security Controls / Policies ...

This program and its output may not be re-sold or copied in any form.

Copyright © Tripex Development Services & NMMU 2012

Home Screen



The Information Security Governance Toolbox Knowledge Base

Knowledge Bases Available

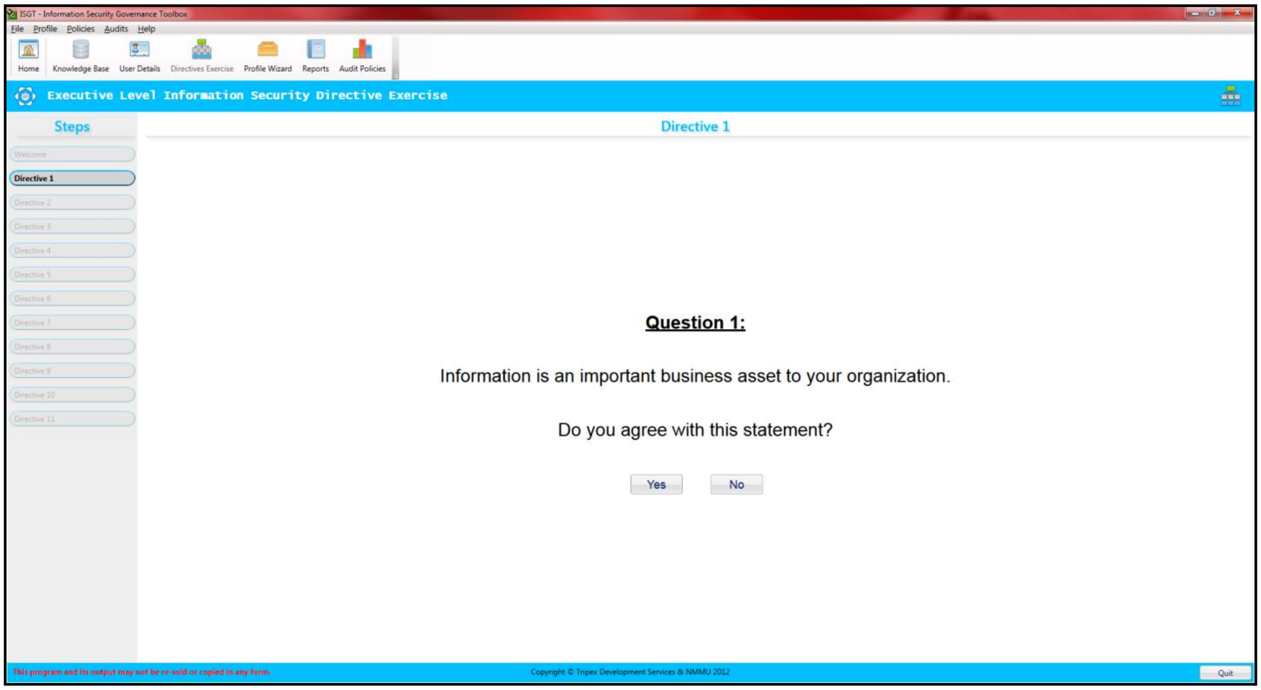
What is Information Security What is an Information Security Management System The Information Security Policy The Information Security Governance Toolbox

1 What is INFORMATION SECURITY?
2 What is INFORMATION SECURITY?
3 What is INFORMATION SECURITY?
4 What is INFORMATION SECURITY?
5 What is INFORMATION SECURITY?
6 What is INFORMATION SECURITY?
7 What is INFORMATION SECURITY?
8 INFORMATION SECURITY MANAGEMENT
9 INFORMATION SECURITY MANAGEMENT

What is INFORMATION SECURITY?

"Quite clearly the information society of the future will just not work if the information we rely on – the lifeblood of a business – is not secured" (Michael Wills, Minister for Small Firms, DTI, UK)

Knowledge Base Component

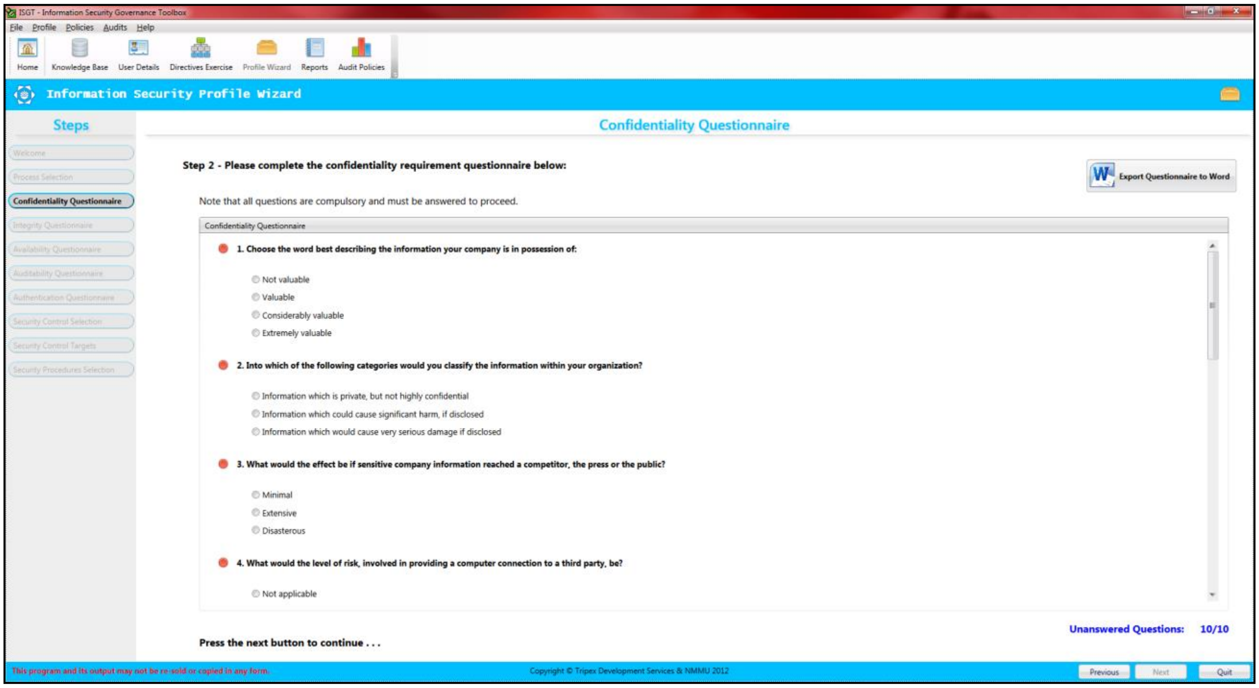

ISGT - Information Security Governance Toolbox
File Profile Policies Audits Help
Home
Knowledge Base
User Details
Directives Exercise
Profile Wizard
Reports
Audit Policies
Executive Level Information Security Directive Exercise
Steps
Welcome
Directive 1
Directive 2
Directive 3
Directive 4
Directive 5
Directive 6
Directive 7
Directive 8
Directive 9
Directive 10
Directive 11
Directive 1
Yes
No
This program and its output may not be re-sold or copied in any form.
Copyright © Tripex Development Services & NMMU 2012
Quit

Question 1:

Information is an important business asset to your organization.

Do you agree with this statement?

Executive Directive Exercise


ISGT - Information Security Governance Toolbox
File Profile Policies Audits Help
Home
Knowledge Base
User Details
Directives Exercise
Profile Wizard
Reports
Audit Policies
Information Security Profile Wizard
Steps
Welcome
Process Selection
Confidentiality Questionnaire
Integrity Questionnaire
Availability Questionnaire
Auditability Questionnaire
Authentication Questionnaire
Security Control Selection
Security Control Targets
Security Procedures Selection
Confidentiality Questionnaire
Export Questionnaire to Word
Confidentiality Questionnaire
This program and its output may not be re-sold or copied in any form.
Copyright © Tripex Development Services & NMMU 2012
Previous
Next
Quit

Step 2 - Please complete the confidentiality requirement questionnaire below:

Note that all questions are compulsory and must be answered to proceed.

1. Choose the word best describing the information your company is in possession of:

○ Not valuable
○ Valuable
○ Considerably valuable
○ Extremely valuable

2. Into which of the following categories would you classify the information within your organization?

○ Information which is private, but not highly confidential
○ Information which could cause significant harm, if disclosed
○ Information which would cause very serious damage if disclosed

3. What would the effect be if sensitive company information reached a competitor, the press or the public?

○ Minimal
○ Extensive
○ Disasterous

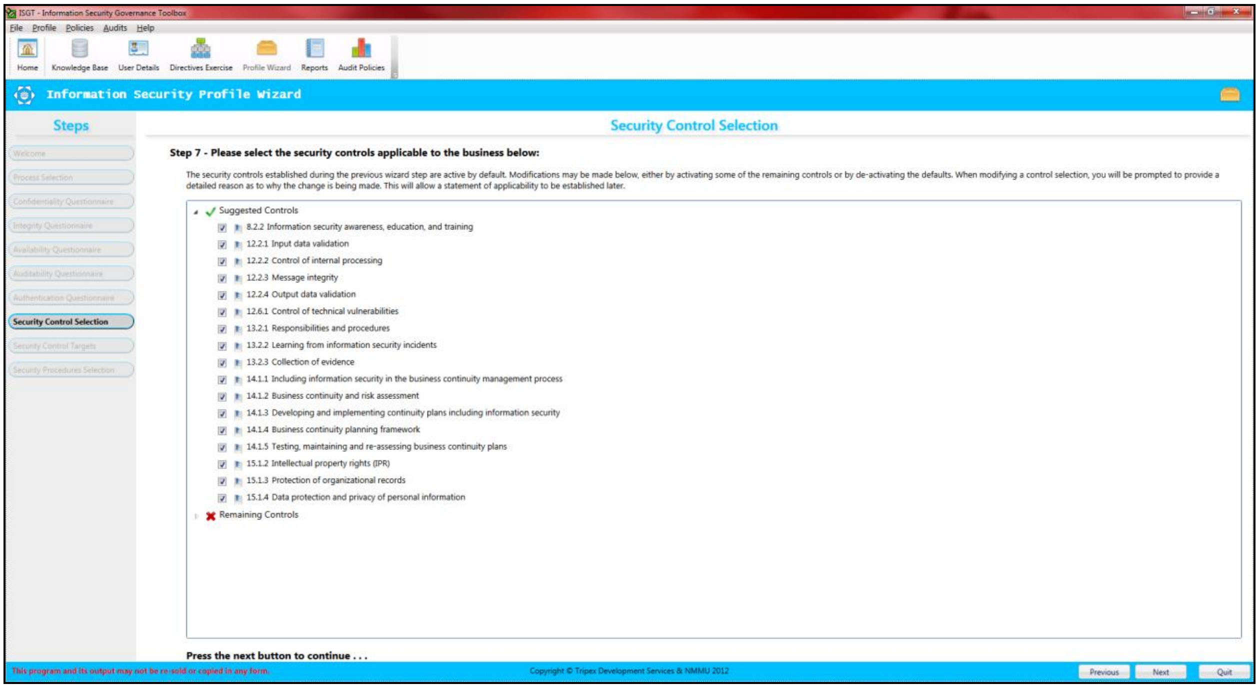
4. What would the level of risk, involved in providing a computer connection to a third party, be?

○ Not applicable

Unanswered Questions: 10/10

Press the next button to continue . . .

Security Requirements Analysis Exercise


ISGT - Information Security Governance Toolbox
File
Profile
Policies
Audits
Help
Home
Knowledge Base
User Details
Directives Exercise
Profile Wizard
Reports
Audit Policies
Information Security Profile Wizard
Steps
Welcome
Process Selection
Confidentiality Questionnaire
Integrity Questionnaire
Availability Questionnaire
Auditability Questionnaire
Authentication Questionnaire
Security Control Selection
Security Control Targets
Security Procedures Selection
Previous
Next
Quit

Security Control Selection

Step 7 - Please select the security controls applicable to the business below:

The security controls established during the previous wizard step are active by default. Modifications may be made below, either by activating some of the remaining controls or by de-activating the defaults. When modifying a control selection, you will be prompted to provide a detailed reason as to why the change is being made. This will allow a statement of applicability to be established later.

✓ Suggested Controls
- ☑ 8.2.2 Information security awareness, education, and training
- ☑ 12.2.1 Input data validation
- ☑ 12.2.2 Control of internal processing
- ☑ 12.2.3 Message integrity
- ☑ 12.2.4 Output data validation
- ☑ 12.6.1 Control of technical vulnerabilities
- ☑ 13.2.1 Responsibilities and procedures
- ☑ 13.2.2 Learning from information security incidents
- ☑ 13.2.3 Collection of evidence
- ☑ 14.1.1 Including information security in the business continuity management process
- ☑ 14.1.2 Business continuity and risk assessment
- ☑ 14.1.3 Developing and implementing continuity plans including information security
- ☑ 14.1.4 Business continuity planning framework
- ☑ 14.1.5 Testing, maintaining and re-assessing business continuity plans
- ☑ 15.1.2 Intellectual property rights (IPR)
- ☑ 15.1.3 Protection of organizational records
- ☑ 15.1.4 Data protection and privacy of personal information

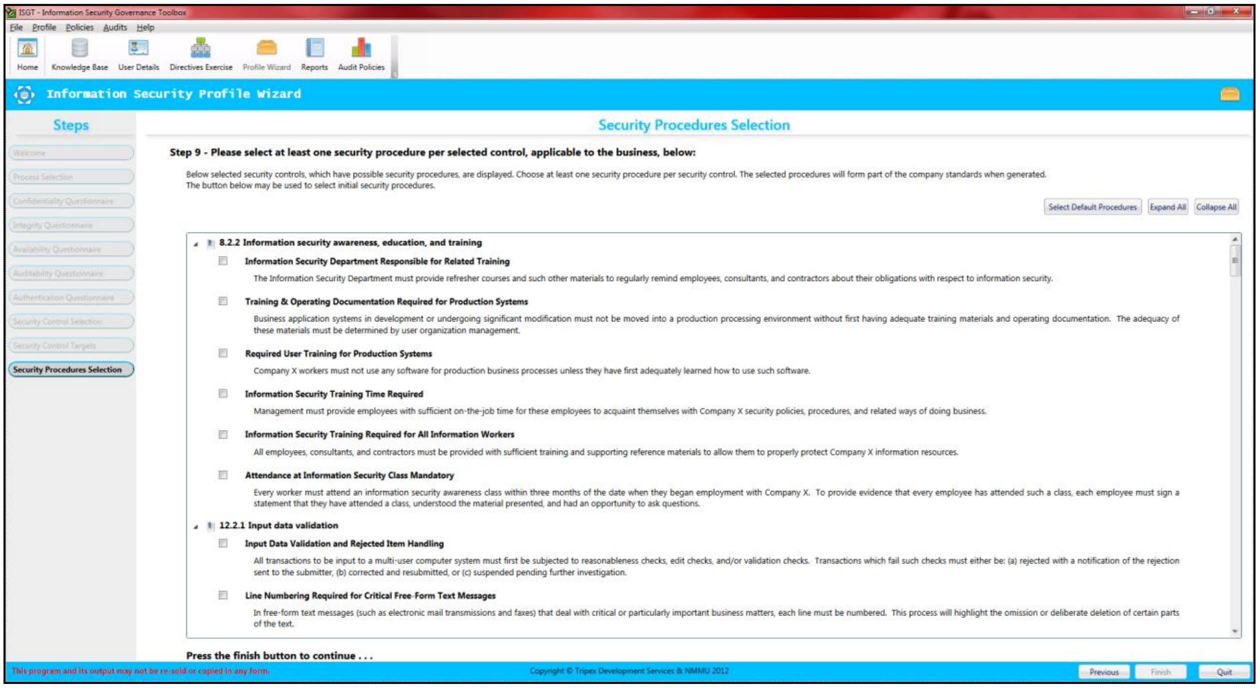
✗ Remaining Controls

Press the next button to continue . . .

This program and its output may not be re-sold or copied in any form.

Copyright © Tripex Development Services & NMMU 2012

Security Control Selection


ISGT - Information Security Governance Toolbox
File
Profile
Policies
Audits
Help
Home
Knowledge Base
User Details
Directives Exercise
Profile Wizard
Reports
Audit Policies
Information Security Profile Wizard
Steps
Welcome
Process Selection
Confidentiality Questionnaire
Integrity Questionnaire
Availability Questionnaire
Auditability Questionnaire
Authentication Questionnaire
Security Control Selection
Security Control Targets
Security Procedures Selection
Select Default Procedures
Expand All
Collapse All
Previous
Finish
Quit

Security Procedures Selection

Step 9 - Please select at least one security procedure per selected control, applicable to the business, below:

Below selected security controls, which have possible security procedures, are displayed. Choose at least one security procedure per security control. The selected procedures will form part of the company standards when generated.
The button below may be used to select initial security procedures.

8.2.2 Information security awareness, education, and training

☐ **Information Security Department Responsible for Related Training**

The Information Security Department must provide refresher courses and such other materials to regularly remind employees, consultants, and contractors about their obligations with respect to information security.

☐ **Training & Operating Documentation Required for Production Systems**

Business application systems in development or undergoing significant modification must not be moved into a production processing environment without first having adequate training materials and operating documentation. The adequacy of these materials must be determined by user organization management.

☐ **Required User Training for Production Systems**

Company X workers must not use any software for production business processes unless they have first adequately learned how to use such software.

☐ **Information Security Training Time Required**

Management must provide employees with sufficient on-the-job time for these employees to acquaint themselves with Company X security policies, procedures, and related ways of doing business.

☐ **Information Security Training Required for All Information Workers**

All employees, consultants, and contractors must be provided with sufficient training and supporting reference materials to allow them to properly protect Company X information resources.

☐ **Attendance at Information Security Class Mandatory**

Every worker must attend an information security awareness class within three months of the date when they began employment with Company X. To provide evidence that every employee has attended such a class, each employee must sign a statement that they have attended a class, understood the material presented, and had an opportunity to ask questions.

12.2.1 Input data validation

☐ **Input Data Validation and Rejected Item Handling**

All transactions to be input to a multi-user computer system must first be subjected to reasonableness checks, edit checks, and/or validation checks. Transactions which fail such checks must either be: (a) rejected with a notification of the rejection sent to the submitter, (b) corrected and resubmitted, or (c) suspended pending further investigation.

☐ **Line Numbering Required for Critical Free-Form Text Messages**

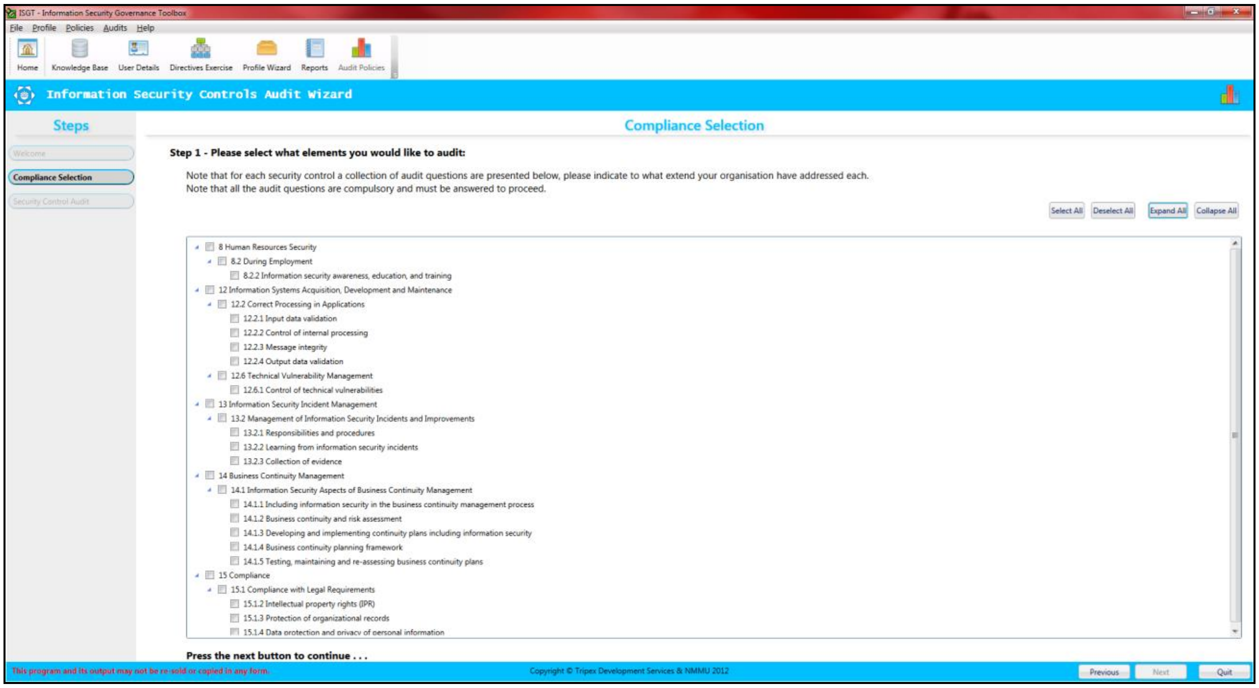
In free-form text messages (such as electronic mail transmissions and faxes) that deal with critical or particularly important business matters, each line must be numbered. This process will highlight the omission or deliberate deletion of certain parts of the text.

Press the finish button to continue . . .

This program and its output may not be re-sold or copied in any form.

Copyright © Tripex Development Services & NMMU 2012

Security Procedures Selection



Compliance Selection

Step 1 - Please select what elements you would like to audit:

Note that for each security control a collection of audit questions are presented below, please indicate to what extend your organisation have addressed each.
Note that all the audit questions are compulsory and must be answered to proceed.

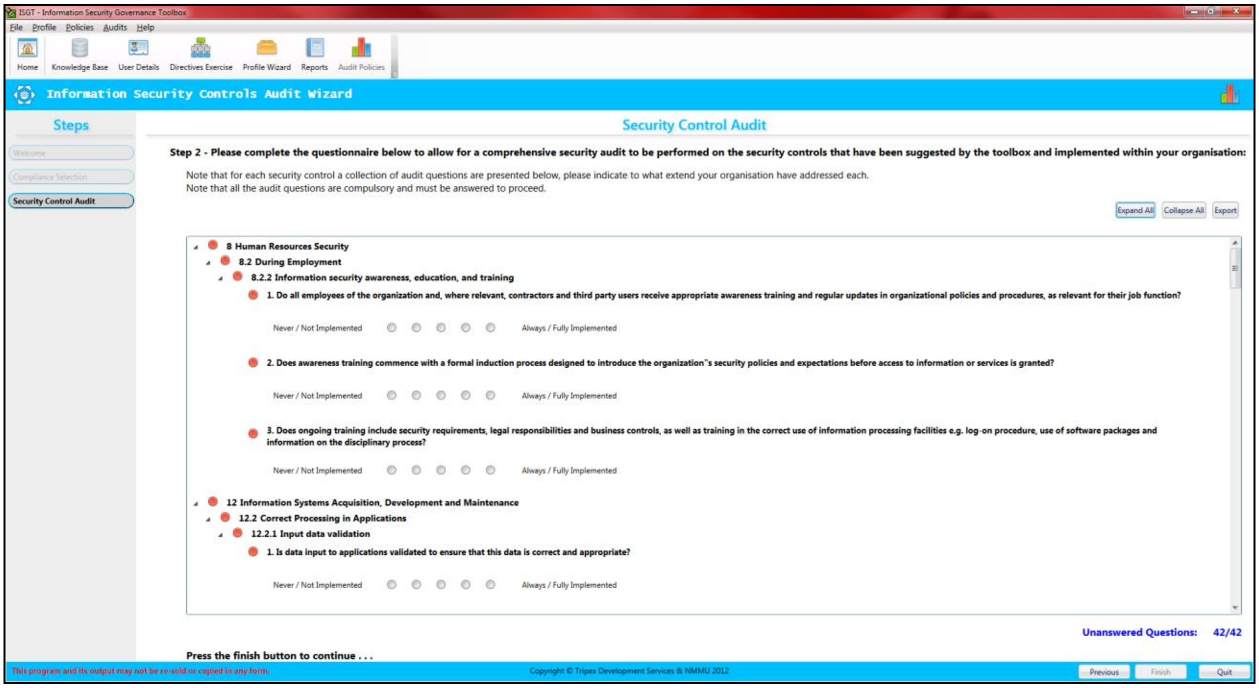
- ☐ 8 Human Resources Security
  - ☐ 8.2 During Employment
    - ☐ 8.2.2 Information security awareness, education, and training
- ☐ 12 Information Systems Acquisition, Development and Maintenance
  - ☐ 12.2 Correct Processing in Applications
    - ☐ 12.2.1 Input data validation
    - ☐ 12.2.2 Control of internal processing
    - ☐ 12.2.3 Message integrity
    - ☐ 12.2.4 Output data validation
  - ☐ 12.6 Technical Vulnerability Management
    - ☐ 12.6.1 Control of technical vulnerabilities
- ☐ 13 Information Security Incident Management
  - ☐ 13.2 Management of Information Security Incidents and Improvements
    - ☐ 13.2.1 Responsibilities and procedures
    - ☐ 13.2.2 Learning from information security incidents
    - ☐ 13.2.3 Collection of evidence
- ☐ 14 Business Continuity Management
  - ☐ 14.1 Information Security Aspects of Business Continuity Management
    - ☐ 14.1.1 Including information security in the business continuity management process
    - ☐ 14.1.2 Business continuity and risk assessment
    - ☐ 14.1.3 Developing and implementing continuity plans including information security
    - ☐ 14.1.4 Business continuity planning framework
    - ☐ 14.1.5 Testing, maintaining and re-assessing business continuity plans
- ☐ 15 Compliance
  - ☐ 15.1 Compliance with Legal Requirements
    - ☐ 15.1.2 Intellectual property rights (IPR)
    - ☐ 15.1.3 Protection of organizational records
    - ☐ 15.1.4 Data protection and privacy of personal information

Press the next button to continue . . .

This program and its output may not be re-sold or copied in any form.

Copyright © Tripex Development Services & NMMU 2012

Company Standards & Security Controls Audit Scope Selection



Security Control Audit

Step 2 - Please complete the questionnaire below to allow for a comprehensive security audit to be performed on the security controls that have been suggested by the toolbox and implemented within your organisation:

Note that for each security control a collection of audit questions are presented below, please indicate to what extend your organisation have addressed each.
Note that all the audit questions are compulsory and must be answered to proceed.

- ● **8 Human Resources Security**
  - ● **8.2 During Employment**
    - ● **8.2.2 Information security awareness, education, and training**
      - ● **1. Do all employees of the organization and, where relevant, contractors and third party users receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function?**

        Never / Not Implemented ○ ○ ○ ○ ○ Always / Fully Implemented
      - ● **2. Does awareness training commence with a formal induction process designed to introduce the organization"s security policies and expectations before access to information or services is granted?**

        Never / Not Implemented ○ ○ ○ ○ ○ Always / Fully Implemented
      - ● **3. Does ongoing training include security requirements, legal responsibilities and business controls, as well as training in the correct use of information processing facilities e.g. log-on procedure, use of software packages and information on the disciplinary process?**

        Never / Not Implemented ○ ○ ○ ○ ○ Always / Fully Implemented
- ● **12 Information Systems Acquisition, Development and Maintenance**
  - ● **12.2 Correct Processing in Applications**
    - ● **12.2.1 Input data validation**
      - ● **1. Is data input to applications validated to ensure that this data is correct and appropriate?**

        Never / Not Implemented ○ ○ ○ ○ ○ Always / Fully Implemented

Unanswered Questions: 42/42

Press the finish button to continue . . .

This program and its output may not be re-sold or copied in any form.

Copyright © Tripex Development Services & NMMU 2012

Company Standards & Security Controls Audit Exercise

Addendum K

Final Evaluation Questionnaire

Business Overview

1. Within which of the below given size classifications do your business fall? (Cross (X) one only)

Size Classification	Employees	Turnover (Million)	Gross Asset (Million)	
Large	Above 200	Above R64	Above R23	
Medium	Up to 200	Up to R64	Up to R23	
Small	Up to 50	Up to R32	Up to R6	
Very Small	Up to 20	Up to R6	Up to R2	
Micro	Up to 5	Up to R0.2	Up to R0.1	
Other				

2. If *other*, please provide a short summary of your business's size classification below:

____

____

____

____

3. How long has the business been in operation? ____________ (years)

Toolbox Simplicity & Cost-Effectiveness Evaluation

1. To what extent was the Toolbox easy to use? (Cross (X) one only)

1	2	3	4	5
Very Poor				Excellent

2. Did your organisation require additional resources to implement and run the Toolbox? (Cross (X) one only)

Yes	No	Don't Know

If *Yes*, please indicate an estimate of the financial expense incurred below:

R ____________________

3. To what extent would you consider the Toolbox cost-effective, when compared to other means for generating information security governance documentation for your business? (Cross (X) one only)

1	2	3	4	5
Very Poor				Excellent

Toolbox Dynamic Document Generation Evaluation

4. To what extent is the output documents generated by the Toolbox usable in your business? (Cross (X) one only)

1	2	3	4	5
Very Poor				Excellent

5. To what extent is the output documents generated by the Toolbox suitable and/or applicable to your business? (Cross (X) one only)

1	2	3	4	5
Very Poor				Excellent

Detailed Dynamic Document Evaluation

6. To what extent are the generated executive-level directives, and its detail, suitable for use in your organisation? (Cross (X) one only)

1	2	3	4	5
Very Poor				Excellent

7. To what extent is the generated corporate information security policy, and its detail, suitable for use in your organisation? (Cross (X) one only)

1	2	3	4	5
Very Poor				Excellent

8. To what extent are the generated secondary-level policies/company standards, and its detail, suitable for use in your organisation? (Cross (X) one only)

1	2	3	4	5
Very Poor				Excellent

9. To what extent is the proposed security controls suitable for use in your organisation? (Cross (X) one only)

1	2	3	4	5
Very Poor				Excellent

10. To what extent is the generated company standard and security control compliance audit report suitable for use in your organisation? (Cross (X) one only)

1	2	3	4	5
Very Poor				Excellent

Toolbox Feasibility Evaluation

11. Did the Toolbox offer assistance, that your organisation otherwise would not have had given the constraints and challenges experienced (e.g. limited resources, experience and expertise)? (Cross (X) one only)

Yes	No	Don’t Know

12. To what extent is the Toolbox feasible for use by businesses similar to your own for generating information security governance documentation? (Cross (X) one only)

1	2	3	4	5
Very Poor				Excellent

Addendum L

Final Evaluation Questionnaire Responses

<u>Question 1:</u>

	Q1.1 Within which of the given size classifications do your business fall? (Micro, Very Small, Small, Medium, Large, Other)	Q1.2 If other, please provide a short description of your business's size classification:	Q1.3 How long has the business been in operation (years)?
Participant 1	Micro	-	55
Participant 2	Small	-	10
Participant 3	Medium	-	100
Average:	-	-	55
Medium:	-	-	55

<u>Question 2:</u>

	Q2.1 To what extent was the Toolbox easy to use? (1 Very Poor - 5 Excellent)	Q2.2 Did your organisation require additional resources to implement and run the Toolbox? (Yes/No/Don't Know)	Q2.3 If yes, please indicate an estimate of the financial expense incurred:	Q2.4 To what extent would you consider the Toolbox cost-effective, when compared to other means for generating information security governance documentation for your business? (1 Very Poor - 5 Excellent)
Participant 1	5	N	-	4
Participant 2	2	N	-	5
Participant 3	2	N	-	3
Average:	3	-	-	4
Medium:	2	N	-	4

Question 3:

	Q3.1 To what extent is the output documents generated by the Toolbox usable in your business? **(1 Very Poor - 5 Excellent)**	**Q3.2 To what extent is the output documents generated by the Toolbox suitable and/or applicable to your business?** **(1 Very Poor - 5 Excellent)**
Participant 1	4	4
Participant 2	4	4
Participant 3	2	2
Average:	3,3	3,3
Medium:	4	4

Question 4:

	Q4.1 To what extent is the generated executive-level directives, and its detail, suitable for use in your organisation? **(1 Very Poor - 5 Excellent)**	**Q4.2 To what extent is the generated corporate information security policy, and its detail, suitable for use in your organisation?** **(1 Very Poor - 5 Excellent)**	**Q4.3 To what extent is the generated secondary-level policies/company standards, and its detail, suitable for use in your organisation?** **(1 Very Poor - 5 Excellent)**	**Q4.4 To what extent is the proposed security controls suitable for use in your organisation?** **(1 Very Poor - 5 Excellent)**	**Q4.5 To what extent is the generated company standard and security control compliance audit report suitable for use in your organisation?** **(1 Very Poor - 5 Excellent)**
Participant 1	4	4	4	4	4
Participant 2	4	4	4	4	4
Participant 3	3	2	2	2	2
Average:	3,7	3,3	3,3	3,3	3,3
Medium:	4	4	4	4	4

Question 5:

	Q5.1 Did the Toolbox offer assistance, that your organisation otherwise would not have had given the constraints and challenges experienced (e.g. limited resources, experience and expertise)? **(Yes/No/Don't Know)**	**Q5.2 To what extent is the Toolbox feasible for use by businesses similar to your own for generating information security governance documentation?** **(1 Very Poor - 5 Excellent)**
Participant 1	Y	4
Participant 2	Y	4
Participant 3	DK	2
Average:	-	3,3
Medium:	Y	4

Comments:

Participant 1:

A super, innovative product which I believe has a lot of potential - especially for smaller organisations that do not have a lot of resources to commit to something like Information Security (but this does not make it any less important for them).

Participant 2:

Using web based technology for the development and use of the Toolbox would be much better. Having to download and install software put hurdles in the way. The process I had to follow throughout the Toolbox was at times not clear. I initially could not work out what I had to do next to access the greyed out sections. I found the slides in the knowledge centre to be basic and not visually appealing. I found the questionnaires a bit simple at times. The user should be given more options, especially for the directives. There was really only one answer to all the questions. I was concerned at times that the Protection of Personal Information Bill (POPI) had not been taken into account. This is the most important applicable law. On the whole, I think the concept is good. It does provide many organisations with a cost effective way to put information security policies in place. And this is crucial considering that information security will soon be required by law (POPI). Better technology (SaaS) could have been used and it could have been better practically implemented.

Participant 3:

I found that the amount of documentation generated was too much. If a company would go with the standard suggestions there would be too many policies and procedures and would actually make management difficult. The documents generated in some cases referred to in my mind outdated technologies as well as the reference to monetary amounts were in $ that will not be relevant to a South African company.

Addendum N

ISSA Paper 2011

A Web-Based Information Security Management Toolbox for Small-to-Medium Sized Enterprises in Southern Africa

Jacques Coertze
School of ICT
NMMU
Port Elizabeth, South Africa
jacques.coertze@gmail.com

Johan van Niekerk
School of ICT
NMMU
Port Elizabeth, South Africa
johan.vanniekerk@nmmu.ac.za

Rossouw von Solms
School of ICT
NMMU
Port Elizabeth, South Africa
rossouw.vonsolms@nmmu.ac.za

***Abstract*—Many small-to-medium sized enterprises are finding it extremely difficult to implement proper information security governance due to cost implications. Due to this lack of resources, small enterprises are experiencing challenges in drafting information security policies as well as monitoring their implementation and compliance levels. This problem can be alleviated by means of a cost effective "dashboard system" and automated policy generation tool. This paper will critically evaluate an existing policy generation tool, known as the Information Security Management Toolbox, and will propose improvements to this existing system based on changes in both information security standards and business needs, since the development of the original system.**

Keywords- computer security, automation, computer software, information security, corporate governance, enterprise security, IT governance, managing information security, methodologies for securing small/medium size enterprises, security policy and procedures.

I. Introduction

Information has become a critical business asset to any organization whether small, medium or large, and forms the life-blood of most organizations [1, p. 408], [2, p. 174]. Information today offers many benefits to an organization such as providing a competitive edge, allowing for economic prosperity or providing real-time reporting [3, p. 25]. There are however many security threats which could compromise information and information technology.

The threats against information and information technology are extensive and the necessity to protect against security threats is more and more eminent. The importance of managing security risks within an organization is very important, providing such protection is one of the key components of corporate governance [4, p. 5], [5, p. 5].

"Corporate governance can be defined as the system (policies, laws, customers etc.) by which an organization is directed and controlled" [5, p. 5]. A sub-component of corporate governance is IT governance that is defined as "consisting of the logical and organizational structures that ensure that an organizations' IT is sustained and extends the business strategy and vision" [6]. Information security is underpinned by IT governance and although a large part of information security governance is located within the realm of IT governance, some parts are found elsewhere as well [4, p. 18].

Information security is implemented within an organization to ensure that threats are mitigated to acceptable levels [7, p. viii]. Information security is a sub-component of information technology governance and, indirectly, of corporate governance [4, p. 18]. Establishing policies and ensuring that the necessary technical and non-technical controls are duly implemented, make up for a large portion of what information security governance and management entails [8, p. 120]. Considerable documentation exists to provide guidance and recommendations on what these controls and policies should entail.

Guidelines and standards have both come into existence to aid in establishing proper information security governance within organizations [7], [9], [10]. The international standard ISO/IEC 27002 [7] focuses most specifically on information security management. It provides for the minimum guidelines of what is expected to ensure proper information security management and it further indicates certain controls and implementation guidelines for an organization. Two guidelines that have grown in popularity are COBIT 4.1 [9] and the King 3 Report for South African based organizations [10]. COBIT 4.1 provides a best practice foundation for information technology governance within an organization and specifies what is expected. It also contains minimal information as to how the implementation should be done. Many South African based organizations are following the King 3 Report's recommendations and it has received considerable focus over the past few years. The above mentioned guidelines do not only apply to large organizations, as small-to-medium enterprises must also familiarize themselves with the contents of the above mentioned guidelines. Overall the general theme portrayed by all of these documents is that policy establishment and monitoring is core to information security governance and that it is vital for top management to provide direction as far as the protection of information is concerned within an organization. Many organizations, in particular small-to-medium enterprises struggle to draft such policies and procedures due to the lack of experience, and in many cases the lack of guidance from a well-qualified information security officer [11, p. 5].

Information security governance dictates that many policies and procedures should be drafted within an organization to ensure that the proper behavior is obtained and dictated to employees to ensure the secure usage of information and related technologies [8, p. 120], [12, p. 275]. This aspect is a huge challenge for small-to-medium enterprises where the financial position of such organizations makes it very difficult to obtain the services of an expert on a part time or full time basis to develop policies and procedures and to guide management [11, pp. 5–6]. As a result, much research has been done in the past to assist these types of organizations in a cost effective and practical fashion with drafting policies and procedures to ensure proper information security governance [8], [13].

This paper specifically addresses the information security management system that was developed on the basis of a framework as proposed by Vermeulen and Von Solms in 2001 [8]. This system was software developed and accordingly documented by Hoppe, Van Niekerk and Von Solms in 2002 [13]. The original system was presented at the 2001 ISSA conference by Von Solms, Gerber, Van Niekerk, Hoppe, Vroom and Aenmey [14]. The paper will critically review the existing system, and the research on which it was based, and will propose changes to the existing work in order to remain current in terms of industry needs. The paper is presented in the form of a case study.

II. Methodology

This paper is presented in the form of a case study. The case study was focused on a particular framework, software implementation and usage of an information security management toolbox. Additionally, literature surveys and some arguing are used throughout the paper.

"Case studies represent intensive, detailed description and analysis of a particular project or program in the context of that project's environment. This makes case studies a valuable way to share the experiences of others who have travelled the road before. Case studies are extremely useful for encouraging discussion about best practices and problem-solving strategies" [15]. Case studies usually follow a specific structure and in this paper the guidelines and structure as set by Cresswell [16, pp. 73–80] will be followed.

The structure set out by Cresswell is as follows:

- Entry vignette;
- Introduction;
- Description of the case and its context;
- Development of issues;
- Detail about the selected issues;
- Assertions; and
- Closing vignette.

This paper will follow the structure of a case study. The next section will introduce the Information Security Management Toolbox. Subsequent sections will continue to describe the particular details of its implementation as well as the framework on which it was based and the limitations that have been identified pertaining to the toolbox will be highlighted and discussed in detail. The paper will conclude with the establishment of a set of criteria to be used for the "next generation" toolbox.

III. Introduction of the Information Security Management Toolbox

An original version of the toolbox was proposed and developed by Hoppe et al. [13]. The original version was demonstrated at the inaugural ISSA conference by Von Solms et al. [14]. This paper forms part of a project which critically reviews the earlier work in light of changes in both security standards and in business needs over the past decade. Hoppe et al.'s essential contribution is the concept that a standalone desktop application can be developed to assist small-to-medium enterprises in proposing the necessary information security policies and procedures as outlined by the mentioned standards and guidelines. It has become known as "The Information Security Management Toolbox" and was designed around the framework proposed for such a system, documented by Vermeulen and Von Solms [13, p. 12]. Both the framework and desktop implementation have become outdated due to the subsequent revision of BS7799 Part 1 and COBIT (due to the frequent enhancements in the information technology environment), but most of the original procedural concepts still apply and can be reused in future implementations.

It should however be noted that many limitations have come into existence due to the change seen within the requirements for small-to-medium enterprises when analyzing the framework and desktop implementation.

The following sections will provide more detail about the toolbox and framework and greater insight into the limitations that have been identified. It will end by providing a set of criteria that can be used for next generation toolbox implementations.

IV. Description of the Information Security Management Toolbox and its Context

As mentioned earlier, the Information Security Management Toolbox developed by Hoppe et al. was based on the framework established by Vermeulen and Von Solms [8]. It must however be mentioned that the toolbox aims at automation of steps within the analysis and development phases of a methodology that was developed by Vermeulen and Von Solms [8, p. 123]. The next section will provide an overview of the methodology and subsequently the framework will be discussed. The section will end with a detailed discussion of the current desktop implementation of the information security management toolbox.

A. The Information Security Management Methodology

The framework proposed by Vermeulen and Von Solms was based directly on a methodology that was created for the establishment and maintenance of an integrated information security management system. A model for it was presented within research in conjunction with the framework [8, p. 123].

The studied methodology is comprised of six phases for the implementation and management of information security, they include:

- Introductory Phase;
- Initial Phase;
- Analysis Phase;
- Development Phase;
- Implementation Phase; and
- Continuation Phase.

These phases form an outline for the implementation of an information security management system. To comprehend the model it is necessary to determine the steps required for the completion of each of the phases and these steps will be identified next.

1) Introductory Phase: The objective of this phase is to put the core elements of information security management into place. These elements comprise the steps that will be required to support the entire information security management process, during its implementation and on an ongoing basis.

The Introductory Phase is comprised of two steps, they include:

- Gain top management commitment; and
- Consult information security standards.

2) Initial Phase: The Introductory Phase is responsible for establishing steps that will contribute towards the introduction of information security. The objective of the Initial Phase is to complete the preparation stage of information security management and allow for its subsequent implementation in the organization.

In the initial phase, the implementation of information security is delegated to lower management. Taking this into account, the steps comprising the Initial Phase are:

- Appoint an information security officer;
- Establish an information security forum; and
- Define security vision and strategy.

3) Analysis Phase: The Introductory Phase and the Initial Phase prepares the organization for implementation of information security management. Having created the foundation for the implementation of information security management, the Analysis Phase begins the process leading up to implementation. The objective of the Analysis Phase is to determine the security requirements of the organization.

The following steps are proposed as necessary for the accomplishment of the goals of the Analysis Phase:

- Determine scope of the ISMS;
- Determine key role players;
- Interview key role players; and
- Determine security requirements.

Once all the above mentioned steps have been successfully completed, the objective of the Analysis Phase has been accomplished, namely to determine the security requirements of the organization.

4) Development Phase: The Analysis Phase identifies the security requirements that define the information security needs of the organization. Proper planning is required to ensure that a well-structured process is followed. For this reason the Development Phase of the proposed methodology is required. The objective of the Development Phase is to evaluate the security requirements and use this information to determine in what way information security management will be implemented in the organization.

The follow steps are proposed to allow for the accomplishment of the above mentioned objective:

- Planning the information security policy structure;
- Information security policy preparation;
- Risk management;
- Procedure preparation; and
- Develop an information security awareness programme.

5) Implementation Phase: Upon successful completion of the Development Phase, the organization is ready for the implementation of some information security management system. The goal of the Implementation Phase is to implement information security according to the guidelines provided by the documents compiled in the previous phase.

Based upon these activities, the following steps are proposed for the realization of the Implementation Phase:

- Empower responsibility framework;
- Implement safeguards according to plan; and
- Offer security awareness programme.

6) Continuation Phase: The previous five phases leads up to the implementation of an Information Security Management System within an organization. It is however vital that support be provided throughout the implementation of information security. For this reason, the Continuation Phase is necessary.

The following steps are proposed to fulfill the Continuation Phase:

- Maintain Information Security Management System;
- Monitor security situation;
- Audit Information Security Management System compliance; and
- Ensure proper incident handling.

The six phases that were described in this section illustrate how an information security management system can be successfully implemented using the proposed Information Security Management Methodology. This is achieved by providing implementation guidance through a structured and phased approach.

Organizations often do not have the expertise or resources to follow such a detailed methodology [13, p. 11]. For this reason Vermeulen and Von Solms established a framework that could be used to create a software tool that can automate steps of some phases within the methodology. The framework proposed will be discussed in the following section.

B. The Information Security Management Toolbox Framework

The framework for an information security management toolbox was presented by Vermeulen and Von Solms [8, pp. 123–125]. The framework was based on the information security management methodology and it was highlighted that the framework helps to automate certain fundamental steps of the analysis and development phases of the methodology.

The first step of the framework is for the users of the toolbox to complete a questionnaire consisting of a series of information security related multiple choice questions in order to conduct some high level business analysis. The degree of information security required by an organization is characterized by security requirements which the questionnaire will identify including confidentiality, integrity, availability, authenticity and audibility.

The results of the questionnaire would then be used to determine the extent of applicability of these five security requirements to the organization. Vermeulen and Von Solms suggested that these security requirements were to be measured according to a qualitative rating of low, medium or high. A weighted calculation process would be applied to the questionnaire and subsequently the ratings of the security requirements could then be calculated.

The second step is to use the calculated/established security requirements and to determine policy statements. Using the framework each security requirement, with its rating of low, medium or high, would cause the selection of one or more policy statements. Within the framework, the relationship between them is determined by using a security requirements/policy statements mapping matrix. The framework would then automate the selection of the policy statements that are to be included as a section of the corporate information security policy document.

The third step is automated and allows the security requirements to determine which safeguards are selected. Each combination of security requirement and rating would have a selection of one or more safeguards associated with it. The collection of safeguards, at the time of writing, was selected to come from BS 7799-1 [17]. Similar to the mapping between the security requirements and policy statement, a mapping matrix exists in the framework to allow for the automated selection of safeguards known as the security requirements/safeguard mapping matrix.

The fourth step is for users to complete a second questionnaire, referring to safeguard elimination. When completed and captured it will evaluate the applicability of certain safeguards by determining the systems and services present in the organization that may affect them. Again this will allow for the automated elimination of certain safeguards and the information concerning the elimination of these is stored in the security requirements/safeguard mapping matrix.

The fifth and last step is highlighted by the framework as being the automated establishment of procedures pertaining to the safeguards selected by the third and fourth step. Each safeguard has a set of one or more security procedures associated with it and the relationship between the safeguards and security procedures are static.

The overall goal of the framework is to automate certain steps of the information security management methodology, which was discussed previously and more specifically to address the automation of proposing of policies and procedures. It must however be mentioned that it is merely a high-level framework/model and is simply a conceptual idea for use by small-to-medium sized enterprises.

Hoppe et al. identified that the framework could be used by a stand-alone desktop application to afford the automation of proposing information security policies and procedures for SME's [13, pp. 11–12]. An implementation was attempted within the same year as which Vermeulen and Von Solms established the framework and a successful prototype was developed for a live-demo at the ISSA conference in 2001 [14]. In the next section the history and implementation details of the application will be discussed.

C. The Information Security Management Toolbox Desktop Implementation

The methodology and framework discussed proposed an implementation model that was used as the basis for the development of an automated software tool to guide the establishment and preservation of information security management in an organization.

The software package carries the working title of the Information Security Management Toolbox (ISMTB). The package provides services in assisting information security management and is an electronic aid providing both interactive elements and textual elements. The content included within the ISMTB was provided by several other research projects [13, p. 17]. The primary objective of the ISMTB is to assist in ensuring the realization of the proposed methodology, thereby effectively addressing the identified security requirements of the organization in a structured and integrated manner. The ISMTB assists in this regard by allowing the automation of the process of identifying and selecting security safeguards and thereby dynamically generating the appropriate security documents required to enforce information security.

The ISMTB was implemented as a stand-alone desktop application using three-tier software architecture within a file sharing environment [13, p. 12]. The primary reason for the architecture was to obtain the benefits of a client/server implementation while executing the ISMTB within a local desktop environment. It must however be mentioned that such a client/server communication architecture was never implemented.

The ISMTB was later provided to a local software development firm to update and in some cases redevelop to conform to best practices in the field of computer programming. Even though the software package was updated in this manner, the actual workings remained the same. The standard on which the ISMTB was based was initially BS 7799 Part 1, but it has subsequently been updated to ISO/IEC 17799 [18]. The questions within the business analysis questionnaire have also been refined over time to be clearer and to map more clearly to the security requirements.

It must be noted that Hoppe et al. did not document in detail the overall workings of the toolbox, although one can argue that the framework provided by Vermeulen and Von Solms described the workings, but the complex mechanisms that were designed to automate the various phases of the proposed methodology has been. Due to this fact the next section will discuss these complex mechanisms.

The ISMTB consists of an introduction module that is responsible for introducing the application users to the concept of information security as well as emphasizing the importance of adhering to a structured and disciplined process when implementing an Information Security Management System. This was implemented using a hypertext approach, presenting the information as a series of hyperlinked web pages that are installed, with the ISMTB, on the client's local desktop environment [13, p. 13].

Although the Introduction module introduces the application users to the concept of information security, it does not provide a means for identifying and proposing a set of security controls. This aspect is implemented in terms of an interactive wizard that serves to automate the steps of the Analysis and Development Phases of the methodology [13, p. 13]. The primary objective of the wizard is to propose a set of modifiable security safeguards to address information security needs of the organization.

For the process of security requirements analysis it was determined that business requirements could be gained using interviews [13, p. 14]. The interviews were to entail key role players within an organization. These interviews would be performed using a high level business analysis questionnaire. Based upon the outcome of the questionnaire, the security requirements would be determined.

Hoppe et al., Vermeulen and Von Solms agreed that in order to assess the importance of security requirements, each security requirement should be referred to by a number of questions in the questionnaire [8, p. 123], [13, pp. 13–14]. Due to this reason a many-to-many relationship exists between security requirements and business analysis questions. The answers selected for each of these questions will determine what rating each associated security requirements will have.

A weighted value system was introduced due to the fact that there is no direct relationship between the ratings of security requirements and the answers of the questions. The weighted value system allows for a calculated process to determine the security requirements for the organization.

Once the security requirements are identified, a series of security controls are presented to the organization. These security controls, as proposed by BS7799-1, are formulated by means of a lookup matrix which maintains a mapping between the various security requirements and their associated security controls. Each security control contains a set of associated security procedures which serve as a guideline for achieving the objectives of each security control. It must however be mentioned that when secondary policies are drafted by the toolbox, that these procedures are all presented. This has led to the confusion that all procedures must be followed and implemented, which may not always be the case.

It was determined that users must be able to select or deselect security controls from the set automatically selected by the toolbox [13, pp. 14-15]. For this reason the toolbox provides an interface that allows users to achieve this, but they must provide a legitimate reason in accordance to the statement of applicability proposed by BS7799-1 when performing such actions.

As mentioned earlier due to changes in the requirements of small-to-medium sized organizations for information security and software development technologies have led to the realization that limitations exist within the framework and toolbox. Now that the background information of the toolbox and framework is known, these limitations will be explored in the following section and a more detailed analysis will follow.

V. Limitations Identified with the Information Security Management Toolbox

The effectiveness of the framework and desktop implemented toolbox has been proven to address the information security management system requirements of small-to-medium sized organizations in the past [8, p. 125]. Today these requirements however have substantially changed and therefore limitations and changes have been identified to fit the current technology framework and business approach.

The framework was aimed towards management of information security. Due to this fact it produced information security policies and procedures based on security requirements established through a business risk analysis. This provides the direct component of governance/management to be present within an organization, but without a control component such a framework is highly limited in its effectiveness today [1, p. 411]. To be effective, a policy must be supported by some way of measuring compliance [1, p. 411], [4, p. 44]. For this reason the framework requires a control component that can assist in this matter. This issue is also present within the toolbox.

The toolbox developed and subsequently updated has seen some minor changes, but the essential functionality offered has remained the same. As mentioned above one of the issues that are present is the lack of a control component, but additional limitations have also been identified with it. It was developed as a stand-alone desktop application for security reasons and it was envisioned that a client/server architecture were to be established. The installation and updating of the application has been identified to be a problem, because individuals using the application need to manually install and update the application. A further limitation is the fact that it is statically developed against the BS 7799-1 standard. Although it has been updated to provide policies and procedures in accordance to ISO/IEC 17799, no effort has been made to afford dynamic changing of the standard. The limitation therefore is that the standard on which it is based cannot easily be changed and the effectiveness of the application has become troublesome. It was originally developed to be used by consultants in the information security field when assisting organizations. Due to cost implications for small-to-medium organizations, and the limited reach of such an approach, it has been decided that a new “self-help” web-based version would be more desirable.

In view of the limitations now identified, the next section will offer an in-depth analysis of these and provide possible solutions or enhancement to mitigate them.

VI. In-Depth Analysis of the Limitations of the Information Security Management Toolbox

It has been clearly mentioned that limitations have been identified with the framework and the information security management toolbox. The aim of this section is to provide a detailed description of each limitation and to propose possible solutions that can be introduced into a “next generation” version of the toolbox. This is regarded as essential to ensure that the current requirements are met for a information security management system in small-to-medium sized organizations.

This section is divided into two subsections, whereby the first portion addresses the framework’s limitations and the second the toolbox’s limitations.

A. The Information Security Management Toolbox Framework

The framework is very comprehensive and has been proven to be effective [8, p. 125]. As already mentioned it offers functionality for automating the proposing of information security policies and procedures, which directs an organization in terms of information security by providing a clear vision and dictating behavior. Although the framework excels in this regard, it does not address any control aspects.

Governance consists of two components namely: directing and controlling [1, p. 409], [5, p. 5]. Directing ensures that a vision is defined and that behavior is prescribed to the parties involved. Control is necessary to ensure that the vision and dictated behavior is followed and if not that corrective actions are taken. For this reason it can be seen essential that the framework incorporates control aspects.

Due to the fact that the framework is based on a standard and automates safeguard selection makes it somewhat simple to introduce aspects of control/compliance. A possible solution that can be followed is to utilize the safeguards and company standards or procedures. Each safeguard and company standards or procedure will dictate that specific information can be captured to determine compliance. Normally such information is included in compliance clauses present within these company standards, the information security policies and statements. Some might require manual capturing methods and other electronic methods. Irrespective the concept would be to capture such information and then to use the standard and company defined compliance specifications to determine whether compliance is being met. Such an approach has been researched and it is envisioned that a similar system can be established for the framework and toolbox implementation.

The analysis and improvement of the current framework forms part of the same larger research project as this paper. However, these issues fall outside the scope of the current paper which focuses specifically on the toolbox itself. It must however be mentioned that future research specifically focusing on the framework itself will be of a high value to bettering the toolbox implementation.

The framework primarily has only one major limitation currently and that has been identified as being compliance measuring and control. The next section will address the limitations of the desktop implemented toolbox.

B. The Information Security Management Toolbox Dekstop Implementation

Many limitations have been identified with the current toolbox implementation. These limitations span from the vision of usage to the computer architecture that was used and beyond. This section aims to provide insight into these limitations.

The previous section outlined that the framework is lacking in providing any control mechanism(s) and this limitation is also present within the toolbox since the inner workings was based upon this framework. As indicated, the safeguard selection and information security procedures and policies can be used to devise a compliance measuring and monitoring system.

For future toolbox implementations it was decided to create a dashboard system that will work in tandem with the proposing of policies and procedures. The dashboard system allows users to enter compliance metrics to indicate what the organization would prefer in order to achieve a specific compliance measurement (as a score out of 10). This information will be captured during the process of safeguard selection and the automation of proposing relevant procedures and policy statements. For each metric a monitoring interval time will be established and when that interval is reached, the dashboard system will indicate that the information for compliance must be gathered. Using the information the dashboard system will prompt the user to enter a rating score out of 10 in respect of compliance. Take note that the dashboard system does not automate the gathering of this information, but simply depends on the manual entry thereof. The overall goal of the dashboard system is to generate simple graph reports for management, which will indicate the current compliance levels versus its information security vision. The result of analyzing such reports will allow management to easily determine whether the organization as a whole is following the vision for information security and to take corrective action where necessary.

The original vision was for consultants to use the toolbox as a tool during one-on-one consultations with organizations. Organizations are experiencing it very costly to hire consultants on a regular basis in order to assist them with their information security requirements [11, p. 6]. For this reason, the cost effectiveness of the current format and use of the toolbox is no longer adequate for small-to-medium sized organizations and a change in the vision of usage is certainly required. This “new” vision is for the toolbox to become an affordable, easy to access, “self-help” tool, that is always up to date in terms of the latest information security standards and controls. Although it can be argued that the current desktop implementation can be adapted to conform to such requirements, the desktop architecture has additional limitations as well which makes it feasible to re-evaluate the architecture. After careful consideration, it was decided to change the current architecture to web application architecture. The web application architecture provides advantages that are not necessarily obtainable by desktop application architecture.

Some of these advantages include [19]:

- No special configuration or changes are needed on user's computers;
- Lower costs;
- Centralized data is secure and easy to backup;
- Updates can be made quickly and easily;
- Information is accessible to a wide audience anywhere in the world;
- Available 24 hours a day, 7 days a week;
- Always up-to-date; and
- Cross-platform capability.

The web application architecture addresses another limitation that was identified with the toolbox. The toolbox installation and maintenance is currently problematic due to the fact that a consultant needs to manually install it onto either his/her own computer or onto an organization's computer(s). This leads to organizations or the consultant using an outdated version, even though a newer version might be available. Mainly this is caused by the fact that there is no centralized access point where updates and installations are stored. In the event of a new version being introduced, the consultant currently has to update the application manually on his own computer and subsequently onto the computer(s) at the organization. Using the web application architecture, this tedious process will in future be eliminated due to the fact that updates to the toolbox will be made at a central location and users accessing the web application subsequently will automatically view the latest updated version. The only problem that might influence the automatic view of the updated version might be when the website is cached on a local server at an organization or on the user's computer, but modern web technologies allow for this to be mitigated to a large extent.

Additionally the web application architecture will offer a user-centric solution for the toolbox, since organizations will have direct access to it. This will also make the toolbox cost effective, since a consultant will not be required on a frequent basis for updating it. This will reduce the dependence on consultants, although the aid that they offer will still be required from time to time. Additionally, the toolbox is currently statically developed against ISO/IEC 17799 [18]. It will be updated to the new revised version of ISO/IEC 27002 [7], but it must be emphasized that the requirement for dynamic changing of the standard is currently a limitation. Currently the toolbox does not offer any means for changing the standard other than changing the actual source code. Design patterns in software development have become very popular and their usage can greatly increase the dynamic nature of the toolbox and assist greatly in future maintenance as well [20]. It is advisable in future that design patterns should be introduced and followed during the web application implementation of the toolbox. This introduces the advantage of dynamically changing the standard on which the toolbox is based and further the maintenance required for the upkeep of the toolbox will be simplified and cost effective.

As indicated by this section, the desktop implementation of the toolbox has some limitations that have come to be known, similarly the framework on which it was based also has a major limitation in terms of compliance monitoring and measuring. It was highlighted that these limitations will be mitigated by means of implementing a newly improved toolbox using web application architecture. The next section will briefly summarize the improvements envisaged as far as the framework and toolbox is concerned and will address criteria to apply to ”next generation” toolbox implementations to ensure that the requirements of small-to-medium sized organizations are embraced.

VII. Criteria for an Information Security Management Toolbox

As discussed in the previous section, improvements are foreseen to be made to both the framework and toolbox. This section will provide a summary of the proposed improvements that will be implemented as well as the key criteria that should be put in place to ensure the successful implementations of the envisaged enhanced toolbox.

The toolbox should be web-based in order to ensure easy maintenance and access to it. Possible technologies that can be used in this matter are: ASP.NET MVC, Silverlight and/or possibly Flash. Overall the goal of changing the architecture to web based architecture will be to allow for a user-centric solution and to address the cost effectiveness of usage thereof.

The need that the toolbox must be part of a larger information security web portal has been identified. The reason for this realization is that the toolbox alone cannot function adequately at addressing all the organizations information security requirements. It is important that a holistic approach is to be followed by means of a web portal to ensure that all aspects of information security are addressed e.g. the introduction process, the awareness by means of training and education, the implementation of policies and procedures and subsequent compliance level monitoring. This can be seen as essential to ensure that the toolbox is not envisaged as being a stand-alone solution for the above mentioned matters, but is an integral part of a larger product.

Due to the fact that a web based solution will be introduced it is envisaged that access to certain areas of the toolbox will have no cost implications, but access to other levels may require a subscription fee in order to cover maintenance and administration costs. This will ensure the toolbox to be cost effective in comparison to acquiring the services of a consultant, hence resulting in more organizations becoming more compliant in the field of information security management.

The following key aspects have now been identified as important criteria to be followed for the future implementations of the toolbox:

- It must be cost effective and user-centric;
- It must be web-based instead of desktop oriented;
- It must be part of a larger information security web portal; and
- Compliance monitoring and evaluation must be implemented.

It is essential that these issues are kept in mind and addressed during the development of future toolboxes to ensure the success thereof at addressing the requirements in respect of information security management of small-to-medium sized organizations.

VIII. Conclusion

To conclude this paper outlined a problem that exists with small-to-medium sized organization where they lack the cost effective resources to implement proper information security management and governance.

It indicated that research was done in the past to assist in this regard and specifically highlighted a framework that was established for the automated proposing of policies and procedures for an information security management system. It continued by providing insight into an information security management toolbox that was developed based on the framework.

Certain limitations were discussed that have been identified with the framework and toolbox due to changes seen in the requirements of small-to-medium sized organization and also in the development technology. These limitations included compliance monitoring and measuring, the development architecture of the toolbox, the vision of usage and usage of design patterns for offering dynamic changes.

Recommendations were made as to how these limitations could be addressed and criteria were provided to be followed in future toolbox implementations to ensure the success thereof. Mainly the proposal entailed changing the desktop implemented toolbox to a web-based application that forms part of a larger web portal. Emphasis was also placed on the fact that future toolbox implementations must be cost effective and user centered.

References

[1] R. Von Solms and B. Von Solms, "Information Security Governance: A model based on the Direct–Control Cycle," *Computers & Security*, vol. 25, no. 6, pp. 408–412, Sep. 2006.

[2] R. Von Solms, "Information security management (1): why information security is so important," *Information Management & Computer Security*, vol. 6, no. 4, pp. 174–177, 1998.

[3] S. Posthumus, R. Von Solms, and M. King, "The board and IT governance : The what , who and how," *South African Journal of Business Management*, vol. 41, no. 3, pp. 23–32, 2010.

[4] S. H. V. Solms and R. V. Solms, *Information Security Governance*. Springer, 2008.

[5] P. Williams, "Information Security Governance," *Information Security Technical Report*, vol. 6, no. 3, pp. 60–70, Sep. 2001.

[6] IT Governance Institute, *Board Briefing for IT Governance*, 2nd Edition. Information Systems Audit and Control Association, 2003.

[7] *Information technology - Code of practice for information security management*, ISO/IEC Std. 27 002, 2005.

[8] C. Vermeulen and R. Von Solms, "The information security management toolbox - taking the pain out of security management," *Information Management & Computer Security*, vol. 10, no. 3, pp. 119–125, 2002.

[9] IT Governance Institute, *Cobit 4.1*. ISACA, 2007.

[10] Institute Of Directors in Southern Africa, *King III Report on Corporate Governance*, Parklands, 2009.

[11] E. Yeniman Yildirim, G. Akalp, S. Aytac, and N. Bayram, "Factors influencing information security management in small- and mediumsized enterprises: A case study from Turkey," *International Journal of Information Management*, Nov. 2010.

[12] R. Von Solms and B. Von Solms, "From policies to culture," *Computers & Security*, vol. 23, no. 4, pp. 275–279, Jun. 2004.

[13] O. A. Hoppe, J. Van Niekerk, and R. Von Solms, *The Effective Implementation of Information Security in Organizations*. Massachusets: Kluwer Academic Publishers, 2002, ch. Information Security Management, pp. 1–18.

[14] R. Von Solms, M. Gerber, J. Van Niekerk, O. Hoppe, C. Vroom, and K. Aenmey, "The information security management toolbox: A practical guide," 2001.

[15] "Case studies," *[WWW document]. URL "http://www.freedomtoaster.org/CaseStudies" Cited 27 April 2011.*

[16] J. W. Creswell, *Qualitative inquiry & research design: choosing among five approaches*, 2nd ed. Sage Publications, 2007.

[17] *A Code of Practice for Information Security*, British Standards Institute Std. 7799-1, 1995.

[18] *Information technology - code of practice for information security management*, ISO/IEC Std. 17799, 2000.

[19] P. Stanley, "Advantages of web applications," *[WWW document]. URL http://www.pssuk.com/AdvantagesWebApplications.htm Cited 26 April 2011.*

[20] E. Freeman, E. Freeman, K. Sierra, and B. Bates, *Head First design patterns*. O'Reilly Media, Inc., 2004.

Addendum M

AfriComm Paper 2012

A Model for Information Security Governance in Developing Countries

Jacques Coertze & Rossouw von Solms

Institute for ICT Advancement, Nelson Mandela Metropolitan University
Port Elizabeth, South Africa
jacques.coertze@gmail.com, rossouw.vonsolms@nmmu.ac.za

Abstract. The proliferation of e-business, e-services and e-governance in developing countries has resulted in businesses and governments becoming highly dependent on business information and related information technologies. Such information is, however, constantly exposed to real threats that could result in security breaches. If these are realised, the prevailing economic structure of a developing country, which is often frail and dependent on the success of its businesses, may be significantly affected as a result of monetary losses. It is thus vital for businesses in these countries to implement, manage and govern information security adequately so as to ensure that valuable information resources are effectively protected. Regrettably, many businesses in developing countries lack the expertise to perform these activities owing to a lack of resources or expertise. Accordingly, the aim of this paper is to establish a model for information security governance that can be implemented with little expertise, as well as minimal effort and capital outlay.

Keywords: information security; corporate governance; enterprise security; IT governance; information security governance; managing information security; security policy and procedures; developing countries

1 Introduction

Information is a critical strategic asset to any business, irrespective of the size [1]. Although businesses continue to reap many benefits from information, in our modern society such benefits cannot be obtained without the help of information technology (IT).

IT is essential to managing the information and knowledge required in the daily operations of a business and thus contributes significantly to its success. Unfortunately, many security threats exist that may compromise information [2]; therefore IT and the information related to it should be adequately protected [3]. This is generally done through a process termed "information security".

Information security pertains to the protection of the confidentiality, integrity and availability of information, which is usually managed by a process called "information security management" [3]. As information and its proper protection are very important to the wellbeing of the modern enterprise, it has become imperative that this be well governed. This is done through a process that is referred to as information security governance [4].

Von Solms [5] defines information security governance as

> consisting of the management and leadership commitment of executive-level management towards good information security; the proper organizational structures for enforcing good information security; full user awareness and commitment towards good information security and the necessary policies, procedures, processes, technologies and compliance enforcement mechanisms, all working together to ensure that the confidentiality, integrity and availability of the company's electronic assets, or information, are maintained at all times.

Many guiding documents, in the form of best practices, guidelines and standards, exist to help in the implementation of information security governance [3, 6, 7]. However, in developing countries, businesses and government departments often lack the expertise needed to interpret and use these guiding documents owing to an absence of resources [8]. This is of particular concern, since these businesses and government departments are now becoming heavily dependent on IT as they integrate electronic services into their daily operations. If the security risks related to such electronic services go unnoticed, it could spell disaster for both them and the economy of the country in which they operate.

Developing countries are thus facing a looming information insecurity tsunami which, if not addressed, could cripple businesses and, ultimately, entire economies [8]. Consequently, the objective of this paper is to establish an information security governance model to assist these businesses in governing their information security activities adequately.

This paper follows a design science research methodology, as outlined by Peffers et al. [9]. Following the methodology, this paper will firstly discuss businesses in developing countries in order to provide an overview of the area of study and to clearly identify a business problem. Secondly, a proposed information security governance model that can be used by businesses in developing countries will be presented. The paper will then conclude by discussing the feasibility of the proposed model.

2 The Business Environment in Developing Countries

Small, medium and micro enterprises (SMMEs) constitute an important part of the business environment in developing countries [10]; consequently, they hold significant implications for society and the environment [11]. Furthermore, SMMEs are labour intensive and therefore make a significant contribution to both the generation of income and the reduction of poverty in developing countries [11].

Many developing countries are rapidly introducing computers and information technology to SMMEs in order to facilitate e-commerce and worldwide service delivery [12]. Furthermore, governments are making more frequent use of e-infrastructure, e-governance and e-services. All of this is creating a high dependence on information and information technology [13]. The concern is, thus, that if the security aspects of this technology and information are not adequately addressed, severe security breaches may occur [3]. These, in turn, may contribute to monetary penalties for SMMEs and governments alike, leading to loss of the income on which the frail economic structure of developing countries is dependent [11]. There is, thus, significant evidence that a definite problem currently exists in the area of information security in SMMEs and the governments of developing countries. This needs to be addressed if these countries are to reap the benefits of their IT investments and enjoy continued economic growth.

The literature on information security [6, 14, 15] recommends that information security should be directed and controlled by executive-level management of SMMEs and government departments. Unfortunately, owing to the limited expertise and resources available in developing countries [10, 16], this level of management in such institutions often does not pay much attention to these duties, as it would rather focus on the operational aspects vital to business survival [8]. Consequently, the security concerns that are inherent in the dependence that is being placed on information and IT are often overlooked.

It can therefore be argued that a solution is required to assist executive-level management of businesses, as well as government departments in developing countries, with information security governance. A contribution in the form of a model for effective information security governance will be outlined in the following section.

3 The Information Security Governance Model

3.1 Principles

The proposed information security governance model is based on the assumption that a lack of expertise exists in businesses and government departments and in the implementation of information security governance, specifically in developing countries. Before such a model can be presented, however, the principles that it should exhibit in order for it to be adopted and implemented successfully have to be made known. Based on the literature, five principles have been established.

Firstly, businesses in developing countries often operate with limited funding and human resources [13, 17]. Moreover, they also have many competing needs [18]. For this reason, a model for information security governance should require minimal effort and capital outlay as well as limited human resources in order for it to be usable and effective.

Secondly, such businesses often cannot afford to hire full-time information security professionals or consultants [17, 19]. In some cases such experts may not even be available [8]. It is therefore vital that the model be presented in an easily understandable format.

Thirdly, as the model addresses information security governance, it should exhibit the actions depicted in the direct–control action cycle established by Von Solms et al. for all forms of governance [14].

Fourthly, the interconnectivity between the input and output requirements of each management level in a businesses should be identified. This will allow businesses to select appropriate tools for generating the inputs and outputs.

Fifthly, the model should facilitate both the *direct* and *control* actions over information security on all levels of management [14]. It should especially address strategic-level management, as this is often neglected in other governance models.

In summary, the principles that need to be exhibited by an information security governance model include the following:

1. It should require minimal effort to obtain the required result.
2. It should be easily understandable.
3. It should be based on the direct–control action cycle.
4. It should identify inputs and outputs at each management level.
5. It should depict complete direct and control activity.

These principles were used to design the information security governance model that will be discussed in the next subsection.

3.2 Model

The information security governance model (see Fig. 1) is based on the direct–control action cycle for information security governance, as outlined by Von Solms et al. [14].

Information security governance operates on three levels of management in a business, namely, the strategic, tactical and operational levels. These three levels are clearly indicated in the model as layers. This is because each management level will generally require different aspects of information security to be implemented – or produced – and monitored in order for proper information security governance to be present.

Similarly, the three actions of governance, namely, *direct*, *execute* and *control,* are also depicted in the composition of the model. These actions provide mutual support and are reinforced by input/output indicators that form the process flow of the model.

The direct action. According to international standards and best practices for information security governance, executive-level management must offer direction and exercise control over information security. Directing starts at the strategic level where executive-level management has to indicate clearly the importance it attaches to the information assets and the way in which such assets contribute to the strategic vision of the business. Such evaluations will need to be based on several factors that may originate from both external and internal sources, including risks, regulatory aspects and business requirements [3]. These factors, in turn, offer input to the security directives that executive-level management should establish.

There are various guidelines that can assist executive-level management in deliberating these factors and establishing directives, for example *Information Security Governance: Guidance for Boards of Directors and Executive Management* [15]. The model facilitates the use of such aids by suggesting that an executive-level directive exercise should be performed (as indicated by (A) in Fig. 1). The output of this exercise will be a set of clearly defined information security directives. These directives will reflect the expectations of executive-level management in terms of information security in the business and will become input to the policies and procedures that should be produced by the lower levels of management. As a result, these directives will contribute to the business's security requirements and policies.

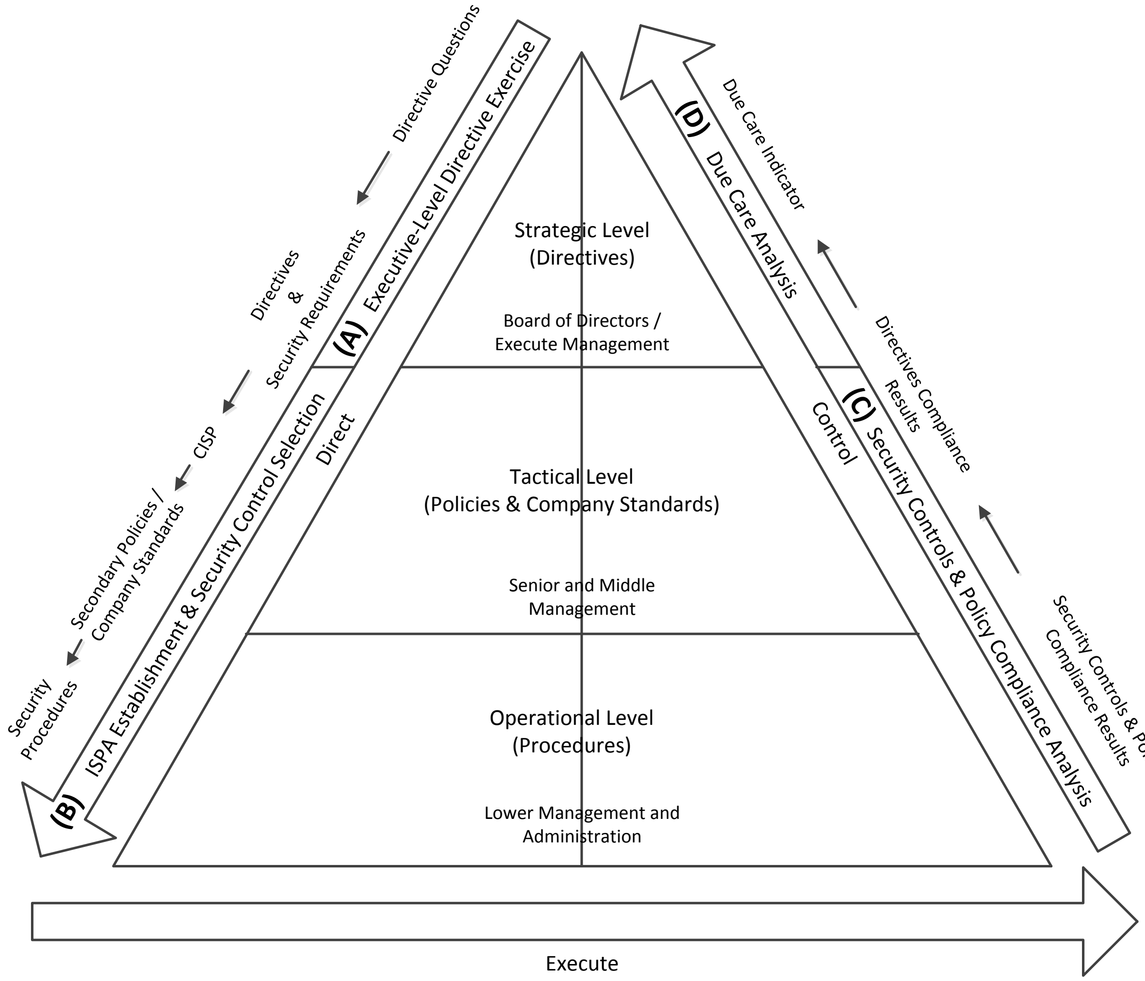

Directive Questions
Directives & Security Requirements
CISP
Secondary Policies / Company Standards
Security Procedures
(A) Executive-Level Directive Exercise
(B) ISPA Establishment & Security Control Selection
Direct
Strategic Level (Directives)
Board of Directors / Execute Management
Tactical Level (Policies & Company Standards)
Senior and Middle Management
Operational Level (Procedures)
Lower Management and Administration
(D) Due Care Analysis
Due Care Indicator
Directives Compliance Results
Control
(C) Security Controls & Policy Compliance Analysis
Security Controls & Policy Compliance Results
Execute

Fig. 1. The Information Security Governance Model

In any business it is vital to determine the applicability and appropriate levels of security requirements. These may include, but are not limited to, aspects such as availability, integrity, confidentiality, auditability and authentication. An existing framework [20, 21] has been developed that supports an adapted risk analysis process for establishing security requirements by making use of a business-oriented questionnaire. In terms of this framework, management is asked a series of security-related questions.

The model proposed in this paper allows for the integration of the existing framework, but indicates that the defined directives from executive-level management should also have an impact on the security requirements. As a result, the responses to the business-oriented questionnaire, together with the directives, should influence the security requirements that are established. These security requirements will consequently govern the content of information security policies and the subsequent selection of security controls. Once these security requirements are known, the model suggests that the drafting of the corporate information security policy may commence.

The corporate information security policy (CISP) can be seen as the cornerstone policy that defines all the high-level security statements that will be applicable to the business. Typically, the CISP will reiterate the directives that have been set by executive-level management, set the scope for the information security policy, specify security roles and specify the vision for information security within the business. The CISP is usually supported by various company standards, which offer further adherence and implementation details to lower levels of management and operational staff.

Company standards generally detail the security controls that have been selected and that will act as the operational security measures in the organisation. A standard that is commonly used for the selection of security controls is ISO/IEC 27002 [3]. This standard offers multiple controls, which may be considered for selection and implementation in a business. Despite the controls offered by the standard, it must be kept in mind that the selection and applicability of security controls will be directly related to the security requirements, the type of business involved and the current state of information security. Further, security controls do not offer procedural guidance or information, and therefore usually need to be supported by security procedures.

Security procedures offer operational guidance for the realisation of security controls. They contain statements that can be followed during day-to-day operations; therefore operational staff depends heavily on such procedures to ensure that a safe and secure environment is maintained.

The model depicts the process for determining security requirements and drafting the security policies and procedures pertaining to the establishing of an information security policy architecture (as indicated by (B) in Fig. 1). As already mentioned, an existing information security management framework [21] allows for this to take place through a semi-automated process based on ISO/IEC 27002 [3].

The model thus demonstrates that the establishing of all the above mentioned components, directives to the information security policy architecture, constitute the *direct* action of information security governance. Unfortunately, adherence to these components per se is not guaranteed, owing to the human nature of employees; therefore, ongoing *control* and *compliance* are vital.

The control action. Proper information security governance can be preserved if ongoing compliance evaluation or monitoring is carried out. Firstly, the security controls and procedures selected and implemented should be checked for usage and adherence by operational staff in the business and, secondly, the duties of executive-level management should be constantly evaluated to determine if due care and due diligence are being exercised with regard to information security.

The *control* action starts at the operational level, where a compliance analysis is performed based on the established security controls (as indicated by (C) in Fig. 1). The compliance analysis aids in determining if the established, or selected, security controls are properly implemented, efficient and effective. This subsequently allows for corrections, or improvements, to be made to the implementation of these security controls.

The model suggests that a policy and security control compliance analysis should be performed by operational and tactical-level management when initiating the *control* action (as indicated by (C) in Fig. 1). In the event that an existing information security management framework is used, a compliance questionnaire consisting of multiple audit questions per security control, based on the auditing guidelines of ISO/IEC 27001 [22] may be drawn up and used for this purpose. Once the compliance analysis has been successfully completed, the results should be used to correct ineffective or unimplemented controls by operational and tactical-level management. Further, the results must be aggregated to the upper management levels for decision making, strategizing and reporting.

To facilitate the decisions of executive-level management, they should receive regular aggregated reports on the implementation and effectiveness of security controls. They also need an indication of whether their own security directives are being met. Further, this level of management should be active in determining their own compliance with legislation, regulations and best practices.

In order to do this, executive-level management should perform a frequent due care analysis (as indicated by (D) in Fig. 1), which will indicate whether due care with regard to information security governance is being taken. In order to perform such a due care analysis a checklist may be used, such as the one established by Von Solms et al. [23]. On completion of a due care analysis, executive-level management will be able to ascertain both possible mismanagement and successful information security governance implementation.

The model depicts this process of policy and security control compliance analysis and due care analysis as constituting the *control* action of information security governance.

The established model can be argued to be feasible and can be shown to be practically viable for businesses in developing countries. This will be substantiated in the following subsection.

3.3 Motivation and demonstration

The model combines numerous concepts, or works, that were established by previous and ongoing research. The aim of the model is therefore to facilitate the grouping of these established ideas. As these ideas are well known and have received great support, it is believed that the model will prove to be feasible and useful. Furthermore, all the concepts portrayed by the model have already been implemented in a prototype software application which may provide additional valuable support for businesses operating in developing countries.

A practical desktop application prototype was developed to demonstrate the feasibility of the model. This prototype is called *The Information Security Governance Toolbox (ISGT)* and is an enhanced version of the existing *Information Security Management Toolbox (ISMTB)* developed during previous research [20].

This prototype facilitates the requirements of the *direct* and *control* action in all management levels of the established model. These include the establishment of security directives, drafting of information security policies and procedures, checking of compliance with these policies and, finally, executing a due care analysis to ascertain whether due care was taken in the information security governance implemented by executive-level management.

It should be noted that a research project is currently underway to evaluate the established model and to improve the current prototype. The findings of the model evaluation and improvements fall outside the scope of this paper, however, and will be presented in future publications.

4 Conclusion

Information is a business asset and has become vital to the successful existence of nearly all businesses. Accordingly, the protection of information is crucial. This protection of information is referred to as information security.

Information security deals with the protection of the confidentiality, integrity and availability of information. Literature on information security recommends that in order for information security to be successful, it has to be well managed and governed.

As a result of a lack of expertise and resources, many businesses in the developing world find it difficult to address the implementation, management and governance of information security adequately. In order to address this problem, this paper presented an information security governance model. In addition, it illustrated the overall actions and workings involved with the concept of information security governance.

The model exhibits five principles, all of which are deemed necessary for the successful implementation of information security governance by businesses in developing countries. The principles include the following:

1. It required minimal effort to obtain the required result.
2. It was easily understandable.
3. It was based on the direct–control action cycle.
4. It identified the interconnectivity between, input and outputs at each management level.
5. It depicted complete direct and control activity.

The objective of establishing an information security governance model that can be used by businesses in developing countries has therefore been met (see Fig. 1).

It should be noted that ongoing research is being conducted to evaluate the established model and to improve the prototype based on it. These improvements and evaluation results will be presented in future publications.

The authors of this paper envisage that the information security governance model will prove highly beneficial to businesses operating in developing countries. Furthermore, since these businesses form such an important part of a developing country’s economic structure, information security researchers should remain vigilant in their attempts to assist them.

Acknowledgements. The financial assistance of the National Research Foundation (NRF) for this research is hereby acknowledged. Opinions expressed and conclusions arrived at are those of the authors and are not necessarily to be attributed to the National Research Foundation.

References

[1] R. Von Solms. Information security management (1): why information security is so important. *Information Management & Computer Security*, 6(4):174–177, 1998. doi: 10.1108/EUM0000000004533.

[2] S. H. Von Solms and R. Von Solms. Information Security Governance. Springer, 2008. ISBN 0387799834.

[3] Information technology – code of practice for information security management. Number 27002. International Organization for Standardization (ISO), 2005. ISBN 978-0-626-21372-5.

[4] S. Posthumus, R. Von Solms, and M. King. The board and IT governance: The what, who and how. *South African Journal of Business Management*, 41(3):23–32, 2010. ISSN 20785976.

[5] S. Von Solms. Information Security: The Fourth Wave. *Computers & Security*, 25(3):165-168, 2006. doi: 10.1016/j.cose.2006.03.004.

[6] Institute Of Directors in Southern Africa. King III Report on Corporate Governance. Institute of Directors in Southern Africa, Parklands, 2009. ISBN 2300000012576.

[7] IT Governance Institute. Cobit 4.1. ISACA, 2007. ISBN 1933284722.

[8] S. Goodman and A. Harris. Emerging markets: The coming African tsunami of information insecurity. *Communications of the ACM,* 53(12):24–27, December 2010. doi: 10.1145/1859204.1859215.

[9] K. Peffers, T. Tuunanen, M. Rothenberger, and S. Chatterjee. A Design Science Research Methodology for Information Systems Research. *Journal of Management Information Systems,* 24(3):45–77, December 2007. ISSN 0742-1222. doi: 10.2753/MIS0742-1222240302.

[10] European Multi stakeholder Forum on CSR. Final results recommendations. Technical report, European Multi-stakeholder Forum on CSR, 2004.

[11] P. Raynard and M. Forstater. Corporate social responsibility: Implications for small and medium enterprises in developing countries. Technical report, United Nations Industrial Development Organization, 2002.

[12] D. Wall. The internet as a conduit for criminal activity. In A. Patavina, editor, Information technology and the criminal justice system. Sage Publications, 2005.

[13] Gupta and R. Hammond. Information systems security issues and decisions for small businesses: An empirical examination. *Information Management & Computer Security*, 13(4):297-310, 2005. ISSN 0968-5227. doi: 10.1108/09685220510614425.

[14] R. Von Solms and S. Von Solms. Information Security Governance: A model based on the Direct/Control Cycle. *Computers & Security,* 25(6):408-412, September 2006. doi: 10.1016/j.cose.2006.07.005.

[15] IT Governance Institute. Information Security Governance: Guidance for Boards of Directors and Executive Management. IT Governance Institute, 2nd edition, 2006. ISBN 1933284293.

[16] O. Perera. How material is ISO 26000 to small and medium-sized enterprises (SMEs). Technical report, International Institute for Sustainable Development, 2008.

[17] C. T. Upfold and D. A. Sewry. An investigation of Information Security in Small and Medium Enterprises (SMEs) in the Eastern Cape. In H. S. Venter, J. H. P. Eloff, L. Labuschagne, and M. M. Eloff, editors, Proceedings of the ISSA 2005 New Knowledge Today Conference, pages 1-17, 2005.

[18] Tawileh, J. Hilton, and S. McIntosh. Managing information security in small and medium sized enterprises: a holistic approach. Proceedings of the ISSE/SECURE, pages 331-339, 2007.

[19] E. Yildirim, G. Akalp, S. Aytac, and N. Bayram. Factors influencing information security management in small- and medium-sized enterprises: A case study from Turkey. International *Journal of Information Management*, November 2010. ISSN 02684012. doi: 10.1016/j.ijinfomgt.2010.10.006.

[20] O. A. Hoppe, J. Van Niekerk, and R. Von Solms. The Effective Implementation of Information Security in Organizations. In Proceedings of the IFIP TC11 17th International Conference on Information Security: Visions and Perspectives, pages 1-18, Deventer, The Netherlands, May 2002. Kluwer, B.V. ISBN 1-4020-7030-6.

[21] C. Vermeulen and R. Von Solms. The information security management toolbox - taking the pain out of security management. *Information Management & Computer Security*, 10(3):119-125, 2002. doi: 10.1108/09685220210431872.

[22] Information technology - Security techniques - Information security management systems - Requirements. Number 27001. International Organization for Standardization (ISO), 2005. ISBN 0-626-17724-3.

[23] R. Von Solms and S. Von Solms. Information security governance: Due care. *Computers & Security,* 25(7):494–497, October 2006. ISSN 01674048. doi: 10.1016/j.cose.2006.08.013.