University of Fort Hare

Together in Excellence

A Process Maturity Assessment Framework of Information Security Policy Development Life Cycle

Tite Tuyikeze

2014

A Process Maturity Assessment Framework of Information Security Policy Development Life Cycle

by

Tite Tuyikeze

201113888

Thesis

submitted in fulfilment of the requirements for the degree

Doctor of Philosophy

in

Information Systems

In the

Faculty of Management and Commerce

of the

University of Fort Hare

Promoter: **Prof. Stephen Flowerday**

December 2014

Abstract

Information security policy development involves more than policy formulation and implementation. Unless organisations explicitly recognise the various steps required in the development of a security policy, they run the risk of developing policies that are poorly thought out, incomplete, redundant and, irrelevant and which will not be fully supported by the users. This study argues that an information security policy has an entire life cycle through which it must pass through during its useful lifetime. A content analysis on information security policy development methods was conducted using secondary sources in the relevant literature. The outcome of the content analysis resulted in the proposal of a framework of information security policy development and implementation. The proposed framework outlines the various steps required in the development, implementation and enforcement of an effective information security policy. A survey of 400 security professionals was conducted in order to evaluate the concepts contained in the framework.

This study also emphasises the importance of integrating a security maturity assessment process into the information security policy development life cycle. A key finding of this study is the proposed maturity assessment framework which offers a structured methodology for evaluating the maturity level of an information security policy. The framework presents an integrated and holistic approach to ensure the incremental process maturity of the organisation's information security policy development process. In addition, organisations using the proposed framework will be able both to determine the current maturity levels of their information security policy development process and also to plan enhancements in the correct sequence.

Keywords: Information security policy development, information security policy implementation, maturity model, maturity assessment

Declaration

I, Tite Tuyikeze, 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.
- This thesis received ethical approval (Ref: FL002 STUY01) from the University of Fort Hare's Research Ethics Committee (UREC).

_____

Tite Tuyikeze

_____01/12/2014_____

Date

Publications

Conference:

Tuyikeze, T. and Flowerday, S.V. (2013). An Information Security Policy Maturity Model (ISPMM). Joint International Conference on Engineering Education and Research and International Conference on Information Technology, Cape Town, South Africa, 8 - 12 December. ISBN: 978-0-9922041-3-6.

Tuyikeze, T. and Flowerday, S.V. (2014). Information Security Policy Development and Implementation: A Content Analysis Approach. Eighth International Symposium on Human Aspects of Information Security and Assurance (HAISA 2014). Plymouth, UK, July 8 - 9. ISBN: 978-1-84102-375-5.

Journal:

Tuyikeze, T. and Flowerday, S.V. (2014). The human factor and information security policy development: The what, how and why? Computers & Security. (Under Review).

Acknowledgements

There is no effortless success; the only way to succeed is through hard work. The journey of a PhD study is not a one day walk which reaches a destination. A considerable amount of effort has been invested by a lot of people in order to accomplish this study. I would like to express my gratitude and appreciation to the following people who have contributed enormously towards the success of this PhD study:

- God Almighty for creating me and giving me strengths and knowledge to complete this study.

- I would like to thank my promoter, Prof. Stephen Flowerday, for the guidance, support and patience throughout this study. Without you, this research could not have been successful. Prof, Thank you very much.

- A special thanks to Prof. Dalenca Pottas, who lectured me in my undergraduate study and supervised my Masters' thesis. Prof Pottas has taught me how to carefully think and logically solve problems. Prof, I have learned a lot from you that have kept me going until today, Thank you very much.

- In memory of my parents, Nyoni Dominique and Niragira Stéphanie; your love, encouragement, support will never be forgotten.

- I am deeply indebted to my family for encouragement and believing in me.

- Prof Eiselen, Thank you for your expert input for the statistical analysis of this study.

- I would like to thank the National Research Foundation (NRF) for giving me the sabbatical grant which enabled me to pay the replacement lecturers who took over my workload while I was on leave to finalise this research project.

- To the thesis editor Mrs Alexa Barnby, your comments were important and I thank you.

Table of Contents

List of Figures

List of Tables

Acronyms

BP	Base Practice
COBIT	Control Objectives for Information Technology
CMM	Capability Maturity Model
Citi-ISEM	Citigroup's Information Security Evaluation Model
DSR	Design Science Research
GISMM	Gartner's Information Security Awareness Maturity Model
GDT	General Deterrence Theory
IS	Information Systems
ISMS	Information Security Management System
ISPA	Information Security Policy Architecture
ISO/IEC	International Organisation for Standardization / International Electrotechnical Commission
ISPDL	Information Security Policy Development Life Cycle
IT	Information Technology
NIST	National Institute of Standards and Technology
OECD	Organisation for Economic Co-operation and Development
PA	Process Area
SSE-CMM	System Software Engineering Capability Maturity Model
SSI	Software Engineering Institute
SPSS	Statistical Package for the Social Sciences
TPB	Theory of Planned Behaviour
TRA	Theory of Reasoned Action
ISPA	Information Security Policy Architecture
ISACA	Information Systems Audit and Control Association
ITGI	Information Technology Governance Institute

Chapter 1: Introduction

Chapter 1
Introduction

↓

Chapter 2
Relationship Between Corporate Governance, IT Governance and Information Security Governance

↓

Chapter 3
Protecting the Security of Information through an Information Security Policy

↓

Chapter 4
Research Design and Methodology

↓

Chapter 5
A Content Analysis of Current Information Security Policy Development Methods

↓

Chapter 6
A Framework for Information Security Policy Development Life Cycle

↓

Chapter 7
Descriptive Statistical Data Analysis and Findings

↓

Chapter 8
Inferential Statistical Data Analysis and Findings

↓

Chapter 9
International Security Standards and Security Maturity Measurement Models

↓

Chapter 10
A Process Maturity Assessment Framework of Information Security Policy Development Life Cycle

↓

Chapter 11
Conclusion

CHAPTER 1: Introduction

1.1 Background

Organisations are extremely dependent on Information Technology (IT) as IT supports their day-to-day transactions and also numerous critical business functions. According to Doughty and Grieco (2005, p. 12), "IT should be seen as a way for increasing the accessibility, speed and comprehensiveness of information that supports the decision-making processes within the organisation." However, the dependency on IT has, unfortunately, resulted in an increase in potential threats to the information assets of organisations (Edwards, 2011).

The findings of the 2014 United States of America survey of cybercrime revealed that more damage was caused by insider attacks as compared to the damage caused by outsider attacks. Insiders comprised the highest percentages of the following incidents: private or sensitive information unintentionally exposed (82%); confidential records compromised or stolen (76%); customer records compromised or stolen (71%), and employee records compromised or stolen (63%) (CERT Insider Threat Center, 2014). Based on the findings of this survey, it is evident that organisations must ensure that they have in place security controls to ensure the confidentiality, integrity and availability of their information (ISO/IEC 27002, 2013).

This study states that one important mechanism for protecting the information assets of organisations is through the formulation, implementation and enforcement of effective information security policies. The literature contains numerous definitions of information security policy. Bulgurcu et al. (2010, p. 2) define information security policy as "a statement of the roles and responsibilities of the employees to safeguard the information and technology resources of their organisations." According to Security Architecture (2008), an information security policy is a set of documents that explains how an organisation will protect both its physical and its electronic assets. On the other hand, Whitman and Mattord (2008) view an information security policy as a document that encompasses established rules that address security issues by providing instructions to the employees as to what they should do when they interact with the information and technology resources of their organisations.

This introductory chapter starts with a description of the problem area under investigation. This is followed by the formulation of the problem statement and research objectives. In addition, the chapter also outlines the research design, research methodology and data collection and data analysis techniques used in the study.

1.2 Statement of the problem

The existing information on security policies found in the literature focuses on the assessment of information security policies in terms of the content and structure. The evaluation of the information security policy itself would have little merit without an assessment of the security policy development process. In addition, there is a lack of evidence as regards a comprehensive and integrated assessment tool with which to assess the processes of the information security policy development life cycle in an organisation. Thus, this lack of evidence, in turn, led to the formulation of the following research question:

Which mechanism should an organisation use in assessing the maturity of its information security policy development life cycle?

This research question implies the following research objective:

1.3 Objective of the study

The main objective of this study is to develop a maturity assessment framework which will provide a structured methodology for evaluating the maturity level of an information security policy. Furthermore, this framework will offer a roadmap for the information security policy development life cycle which will promote sustainability.

In order to realise the main research objective mentioned above, the following secondary objectives will also need to be addressed:

a. Discuss the importance of implementing effective information security policies and then introduce these policies as important facets of governance;
b. Determine the major processes required in formulating, implementing and adopting effective information security policies;
c. Investigate the importance of the information security policy development life cycle from the security professionals' view point;

d. Determine whether there is a relationship between the management support, employee support and the information security policy development life cycle;
e. Investigate existing security maturity measurement models and their role in assessing an organisation's information security management;
f. Identify the key characteristics that are necessary in order to assess the maturity of the information security policy development and implementation processes.

1.4 Significance of the study

The existing literature concentrates on a description of the structure and content of the security policy, but, in general, it fails to describe in detail the processes which are used to generate the output of the information security policy. Consequently, information security policy development staff members experience difficulties concerning the processes they should follow during the information security policy development and implementation.

In view of the lack of available guidance for developing information security policies, security policy developers often use other organisations' policies, commercially available sources and/or templates available from public sources, such as the internet, to find answers to their questions. However, the resulting document will not provide proper direction for the information security within the context of the organisation that it is supposed to protect. In such case, the policy statements developed may not be directly applicable to the risks they are designed to mitigate and, thus, they will not combat the security threats that the specific organisations are facing. McKenna (2010, p. 5) states that: "unfortunately, many IT security people do not understand business IT alignment, so they end up writing these huge security policies that are all about protecting everything."

In addition, there is lack of a comprehensive and integrated assessment tool which may be used to evaluate the processes involved in developing and implementing information security policies. It is therefore, in response to this gap in the literature that this study proposes a framework that will provide a comprehensive, structured methodology for assessing the maturity level of an information security policy. The framework should provide an evolutionary path from an ad hoc, information security policy development approach to a more structured, defined, manageable and repeatable quality approach that both protects the critical information of organisations and allows for milestones to be created, measured and met in a projected manner.

1.5 Initial literature review

Threats to corporate information are constantly increasing at a time when businesses are relying more heavily upon Information Technology (IT) than ever before. However, despite the fact that this dependency on IT assists organisations to reach their business objectives, it also exposes their information to numerous security risks and threats. Tokhid, Abdul-Rashid, and Abdul-Roni (2012) and Dzazali, Sulaiman and Zolait (2009) claim that organisations that depend on IT are facing a continuous increase in the number of types of risk that are no longer limited to the compromise of the information system network but also include legal liabilities such as human errors, loss of trust , and severe financial repercussion. Although an organisation may have effective technical controls in place, the human factor remains the weakest link in comprehensive information security management (Etsebeth, 2006). Those people who cause either intentional or unintentional threats to organisations are referred to as insider threats (Richardson, 2009).

According to Schultz and Shumway (2001, p. 7), an insider threat is “the intentional misuse of computer systems by users who are authorised to access those systems and networks.” The literature review indicates that both intentional and unintentional insider threats have been considered to be one of the top ranked threats to information security over the past decade (Richardson, 2009).

The CyberSecurity Watch Survey (2011) found that the damage caused by insider (employees or contractors with authorised access) attacks was more extensive than the damage caused by outsider (those without authorised access to network systems and data) attacks. The most common insider e-crime included: unauthorised access to corporate information (63%); unintentional exposure of private or sensitive data (57%); virus, worms, or other malicious codes (37%), and theft of intellectual property (32%). “Not only are insider attacks monetarily costly, but they also cause additional harm to organisations that can be difficult to quantify and recoup. Harm to an organisations’ reputation, critical system disruption and loss of confidential or proprietary information are the most adverse consequences from insider cybersecurity events” (CyberSecurity Watch Survey, 2011).

Both researchers in the information security management field and also practitioners are of the opinion that an effective information security policy constitutes the main control in mitigating the insider threats (Talbot and Woodward, 2009; Karyda, Kiountouzis and Kokolakis, 2005). An information security policy should ensure that authorised

employees only are able to access the organisation's network and information resources (Whitman and Mattord, 2008). According to Heikkila (2009), an information security policy should inform employees about the penalties and consequences of the inappropriate use of an organisation's information assets. Nevertheless, although the implementation of a comprehensive information security policy has numerous benefits for organisations, the processes of developing, implementing and adopting an effective policy are difficult at best.

The existing literature on information security policy development and implementation suggests the basic steps for the development of a security policy document. The informal comparison between existing information security development and implementation methods conducted in this study revealed some similarities with the writers agreeing on the same steps but, also gaps in terms of a particular writer would not having mentioned a particular step that the others considered important. It was in light of these gaps in literature that this study conducted a content analysis of existing information security policy development and implementation in order to formulate the processes required for developing an information security policy.

In addition, there is a lack of guidance concerning the assessment of the information security policy development and implementation processes. Consequently, one of the aims of this study is to integrate security maturity assessment into the security policy development using a maturity model approach. Accordingly, the study investigated current security maturity models in order to ascertain the best approach that may be used to assess and guide this process. A maturity model is a structured collection of elements that describe certain aspects of maturity levels in an organisation (Eshlaghy and Pourebrahimi, 2011). Inspired by the ISO/IEC 21827 and COBIT 4.1 maturity models, the study proposed a process maturity assessment framework for the information security policy development life cycle. The next section discusses the research design and methodology used in the study.

1.6 Research design and methodology

Leedy and Ormrod (2005, p. 114) define research design as the stance taken by the researcher in order to investigate an existing phenomenon with the aim of providing solutions to the phenomenon observed. This section describes the plan that was used to conduct this research project. It also highlights the philosophical stance underlying the study as well as, the research paradigm, research method, research design and data collection methods used.

1.6.1 Research paradigm

In any research, the researcher seeks to elicit new knowledge or facts in a systematic or organised manner in order to increase the existing body of knowledge (Saunders, Lewis and Thornhill, 2009, p. 119). This task starts by the careful selection of a research topic, area of interest and a research paradigm. A research paradigm is a network of coherent ideas about the nature of the world and the functions of the researchers which are adhered by a group of researchers, conditions their thinking and underpins their research actions (Bassey, 1990).

Collis and Hussey (2009, p. 58) maintain that there are two research paradigms: positivism and interpretivism. According to Saunders (2009, p. 119), there are four philosophical paradigms that may be used in IT research: positivism, interpretivism, realism and pragmatism. Livari (2007) and Vaishnavi and Kuechler (2008) argue that Design Science is emerging as a research paradigm in the building of IT artefacts.

Collis and Hussey (2009, p. 69) argue that the paradigm adopted for a study is influenced by the dominant paradigm in the research area and the nature of the problem under investigation. In order to answer the research question posed by this study, this research project followed the pragmatism paradigm which supports the mixed method approach. The mixed method combines both qualitative and quantitative approach. Firstly, this study adopted a qualitative approach during the content analysis of existing theories and methods of developing information security policies. Based on the results of this content analysis, a conceptual framework was developed. Secondly, this research study used a quantitative approach to validate the reliability of the proposed framework constructs. The study also followed the Design Science paradigm. Design Science provides comprehensive guidelines for the designing of IT artefacts (Hevner et al., 2004).

1.6.2 Research approach

The research philosophy adopted in this study was supported by the inductive reasoning approach. According to Martin (1997) and Trochim (2001), inductive reasoning begins to detect patterns and regularities, formulates certain tentative hypotheses that may be explored and culminates in developing some general conclusions or theories. This study used inductive logic to study the relevant literature available on existing information security policy development processes. The literature review, combined with the feedback from the expert review, resulted in the formulation of the framework.

1.6.3 Research design

This study followed the Design Science guidelines in producing and evaluating the output or solution. According to Peffers et al. (2008, p. 49), Design Science research involves "a rigorous process to design artefacts to solve observed problems, make research contributions, evaluate the designs, and communicate the results to appropriate audiences." The literature indicated various approaches that researchers and practitioners may use in designing and evaluating IT artefacts (Hevner et al., 2004; March and Storey, 2008; Baskerville et al., 2009; Gregor and Jones, 2007; Peffers et al., 2008). This study adhered to the most widely cited guidelines of Design Science as proposed by Hevner et al. (2004). Hevner et al. (2004) suggest seven guidelines that describe the characteristics of a well-executed Design Science project.

1.6.4 Research methods

According to Creswell (2009), there are three research methodologies, namely qualitative, quantitative and mixed method. Marshall and Rossman (2010) maintain that qualitative is a descriptive and interpretive method of gathering and analysing data. On the other hand, Offerman et al. (2009) states that quantitative technique assesses the characteristics of the evaluation object on a numerical basis. However, Creswell (2009) recommends the use of mixed method research and this type of research combines both the qualitative and quantitative forms of research and mixes them in order to strengthen the study. This study used a mixed method research methodology and, thus, it used both qualitative and quantitative methods during the data collection and data analysis processes.

1.6.5 Data collection

This study used a mixed method exploratory sequential design. The exploratory sequential design begins with and prioritises the collection and analysis of qualitative data (Creswell, 2009). Building on the exploratory results, the researcher then conducts the quantitative phase of the research in order to test or generalise the initial findings. Firstly, the exploratory sequential design adopted in this study explored the different processes used in developing and implementing information security policies as found in the literature using a content analysis technique. The results of the content analysis were used to construct a conceptual framework for the information security policy development life cycle. Secondly, quantitative data was collected in order to evaluate the framework's

constructs with the objective of generalising the findings. Figure 1.1 depicts the exploratory sequential design of this study.

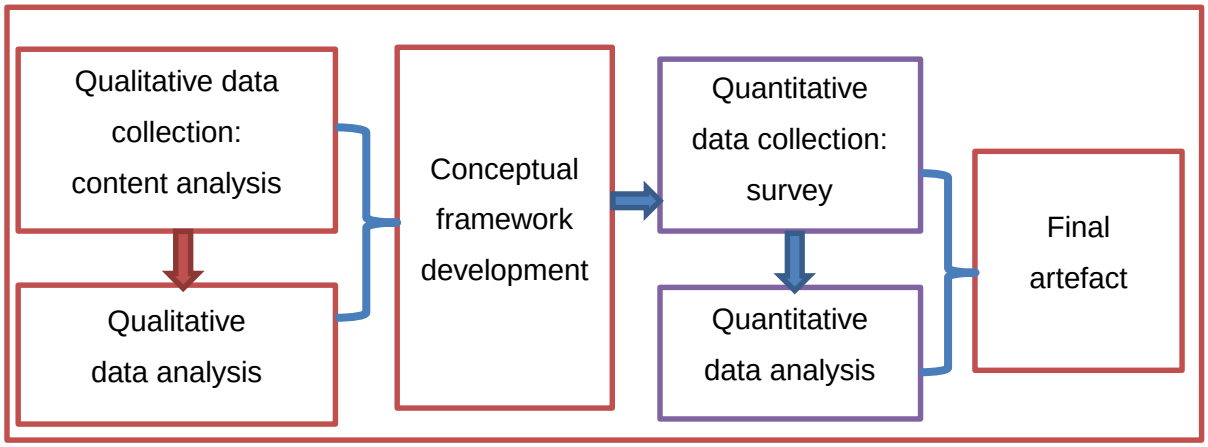


Figure 1.1: Exploratory sequential design (Creswell, 2009)

The next section discusses the data analysis used in the study.

1.6.6 Data analysis

The data analysis followed the triangulation process which combines both qualitative and quantitative data. Saunders et al. (2009, p. 145) define triangulation as "the use of two or more independent sources of data-collection or analysis methods within one study in order to help ensure that the data is telling you what you think they are telling you." The use of a combination of data types (triangulation) increases the validity of a study as the strengths inherent in one approach may compensate for the weaknesses inherent in another approach (Voce, 2005). Figure 1.2 depicts the data triangulation applied in this study.

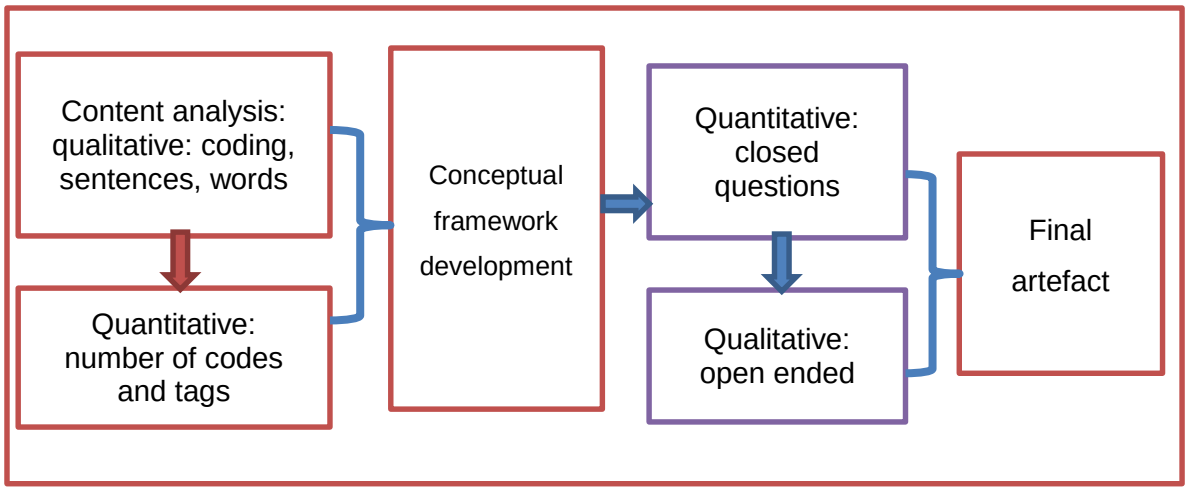


Figure 1.2: Data triangulation (Saunders et al., 2009)

As illustrated in Figure 1.2, which depicts the quantitative and qualitative data collection, both narrative and numeric data were analysed. The qualitative data collection was conducted using the content analysis research technique while the Statistical Package for Social Science (SPSS) was used to analyse the quantitative data which had been collected. Descriptive statistical tests were used to generate the mean, median and standard deviation. Cronbach's Alpha was used to measure the reliability of the questions. Inferential statistical tests were also used. Pearson's correlation coefficient was used to investigate the relationship between the constructs of the information security policy development life cycle. The next section discusses the ethical considerations of the study.

1.7 Ethical considerations

Research ethics involves identifying the morally accepted code of conduct in conducting research (Babbie, 2005). The ethical approval to conduct the study was given by the University of Fort Hare's Ethics Committee (attached in Appendix A). The respondents who participated in the survey were provided with sufficient information to inform them about the objective of the study. Their consent to participate in the study was obtained while they were also informed of their right to withdraw from the study at any time. The data that was collected during the survey remained confidential and was not used for any purpose outside of the aim of the study.

1.8 Key findings of this research project

In order to realise the main research objectives and sub-objectives of the study, a content analysis of existing information security policy development and implementation methods was conducted in order to gain an in depth understanding of the processes involved in the information security policy development life cycle. Based on the results of the content analysis, a conceptual framework of information security development life cycle was proposed. The proposed framework was then refined based on the suggestions of professionals from the survey and from the expert review feedback. The refined framework comprises five dimensions that constitute the main pillars of the information security policy development and implementation process.

The first dimension is the **information security policy development life cycle.** It encompasses the processes needed to develop an information security policy: risk assessment; information security policy construction; information security policy

implementation; information security policy compliance, and information security policy monitoring and review.

The second dimension is the **security policy drivers** as it is composed of threats that put the organisation under pressure to have mechanisms in place to protect their information. Abdel-Aziz (2010) states that "before discussing information security policy and the process to assess it, it is important to know what drives information security in the first place." The development of information security policy is driven by external and internal factors that put the organisation under pressure to have mechanisms to protect organisations' information. These are internal threats such as employees who put the organisations' information at risk and external threats such as hackers, crackers, virus, etc. Moreover, there is compliance with the increasing government legislation requirements.

The third dimension is the **security policy guidance**. This is constituted by security standards that guide organisations in constructing an information security policy. International security standards such as ISO/IEC 27002 constitute a major guide to follow during the development of an information security policy.

The fourth dimension is the **people support dimension**. This dimension includes the people that are involved in the development of an information security policy. Management, employees and stakeholders need to support the whole process of developing and implementing an information security policy in order for it to survive and attain its objectives.

Lastly, the organisations need to use **existing theories** to understand the employees' behavioral intention with regards to information security policy compliance. This study relies on the Theory of Planned Behaviour and General Deterrence Theory in order to understand the employees' behavioural intention to comply with organisations' security policies.

A survey of 400 security professionals was conducted in order to evaluate the concepts of the framework. The results of the survey revealed that, in the main, the respondents agreed that all seven constructs of the proposed framework are important. In addition, the overall results showed that risk assessment was the most important construct of the seven measured constructs.

Furthermore, the content analysis revealed a high frequency of occurrence of management support and employee support in the results of the content analysis.

Accordingly, it was assumed that it is essential that management support and employee support are involved in all the processes of developing and implementing information security policy. In addition, inferential statistical tests were conducted to ascertain whether there is a relationship between management support and the information security policy development life cycle constructs. The findings showed a positive correlation between management support and information security policy development life cycle constructs with a statistically significant result.

In the same vein, an assumption was made that it is essential that employee support is involved in all the information security policy development life cycle constructs. Inferential statistical tests were used to ascertain whether there is a relationship between employee support and the information security policy development life cycle constructs. The findings confirmed the existence of a relationship with significant influence between employee support and information security policy development life cycle constructs. Therefore, the findings confirmed the assumptions that had been made and the results were then applied to the proposed framework.

In addition, a framework to assess the processes of information security policy development and implementation was proposed based on the ISO/IEC 21827 and COBIT 4.1 process maturity levels. The next section discusses the outline of the chapters contained in the study.

1.9 Outline of proposed chapters

Chapter 1 is an introductory chapter and it includes a discussion of the background to the study, the identification of the research problem and an outline of the research objectives and the research methodology that were used in the thesis.

Chapter 2 discusses the relationship between Corporate Governance, IT Governance and Information Security Governance. The chapter also highlights the importance of implementing effective information security policies and then introduces such policies as an important facet of governance.

Chapter 3 deals with the challenges pertaining to the development and implementation of an effective information security policy. The chapter also presents the theories underlying information security policies.

Chapter 4 discusses the research methodology used in the study including the philosophical perspective, research approach, research strategies, and data collections and data analysis methods.

Chapter 5 discusses the content analysis of relevant literature that was conducted in order to acquire a detailed understanding of the existing information related to security policy development and implementation methods.

In **Chapter 6**, the results of the content analysis combined with the feedback from expert reviewers delved into the creation of the framework.

Chapter 7 concentrates on the discussion of the descriptive statistical data analysis and findings.

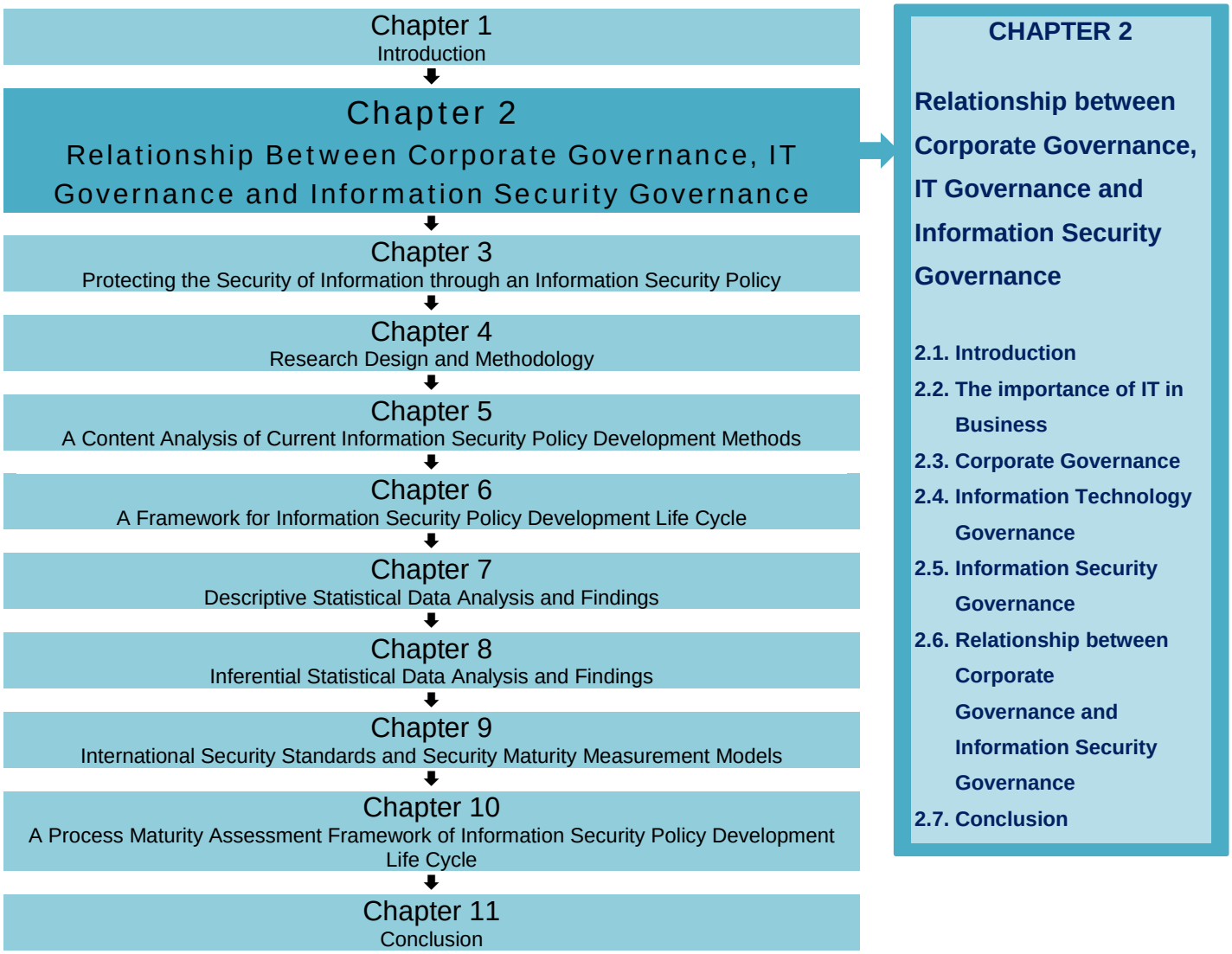
Chapter 8 discusses the inferential statistical data analysis and findings.

Chapter 9 investigates the current international standards and security maturity measurement models.

Chapter 10 proposes a process maturity assessment framework of the information security policy development life cycle.

Chapter 11 presents an overview of the study, the conclusions and limitations of the research and recommendations for further research.

Chapter 2: Relationship between Corporate Governance, IT Governance and Information Security Governance



2.1 Introduction

The objective of this chapter is to highlight that there is currently an increase of the use of Information Technology (IT) within organisations in order to carry out daily transactions. However, although IT assists organisations to attain their business objectives and goals, it also exposes their information to numerous security risks and threats.

This chapter emphasises that the executive management of an organisation is compelled to be committed to and responsible for information security in terms of law and also to ensure good Corporate Governance within the organisation. Corporate Governance requires organisations to have in place an effective information security management plan to protect their information. An organisation's information is considered to be its most valuable asset. As stated by Von Solms and Von Solms (2005, p. 11), "…the data and information of the business have become its "life blood" and compromising this life blood could "kill" the business." This chapter also aims to establish a direct relationship between Corporate Governance, IT Governance and Information Security Governance.

2.2 The importance of IT in business

In today's competitive business environment, organisations depend on information to enable them to carry out their daily business activities. However, this dependency has grown to a point at which most organisations are not able to function effectively without access to Information Technology (Tokhid et al., 2012). Von Solms and Von Solms (2006) maintain that business information and the systems processing such information have become key assets in most organisations today. According to Doughty and Grieco (2005, p. 9), "IT should be seen as a way for increasing the accessibility, speed and comprehensiveness of information that supports the decision-making processes within the organisation."

IT is being used in almost all organisations, whether they are manufacturers, consultants, governmental agencies, or other entities. IT is also used to store and manage the large amount of information on which organisations depend in order to carry out their daily activities. Gantz, Chute, and Manfrediz (2008) estimate that, in 2007, the amount of information created and captured in digital form exceeded 281 exabytes. According to Von Solms and Von Solms (2006, p. 5), "information is the glue that tightens the whole organisation together and enables close communication between the organisation, its clients and external stakeholders."

The development of private IT networks and the widespread utilisation of the Internet have facilitated the way in which organisations can carry out business transactions with their customers, suppliers and other business partners (Gantz et al., 2008). However, "the proliferation of computer networks and the advent of the internet have added another dimension to information security" (Tokhid et al., 2012, p. 6). Nowadays, it is amazing to consider how the use of the internet affects our daily lives. For many people, it is difficult to imagine life without internet browsing, email and texting, online shopping, smartphones, social media, digital entertainment, and online banking and account payment. According to DTTL (2011, p. 26), "given how much our modern lives now revolve around information and connectivity, it is scarcely an exaggeration to think of information security as a matter of life and death."

Although the use of IT offers numerous advantages to business growth, organisations face significant challenges as regards protecting their information assets within a complex and changing environment (Hardy and Williams, 2010). An organisation's information may be stored in multiple types, forms and formats (e.g. traditional documents, text messages, video, email, audio etc.) within diverse systems and technologies (e.g. databases, documents, social networking tools etc.). In addition, it is possible for an organisation's information to be accessed by outsiders who are not under the direct control of the organisation, for example, software service providers, outsourcing and cloud computing. This, in turn, makes it, difficult to ensure the privacy and security of such information.

Tokhid et al. (2012) highlight that organisations that depend on IT constantly face an increased number of risks such as the compromising of the system network, human errors, loss of trust and severe financial loss. In addition, organisations are also obliged to comply with the numerous legal and regulatory requirements which are mandated at the national as well as the international level. It is, thus, essential that an organisation's IT is well managed and governed to ensure the survival of the organisation in this competitive era. De Haes and Van Grembergen (2008, p. 32) state that "the pervasive use of technology has created a critical dependency on IT that requires organisations to have in place an efficient IT Governance strategy. This strategy consists of the leadership, organisational structures and processes that ensure that the organisation's IT sustains and extends the organisation's strategy and objectives."

Senior managers in both corporate and public organisations are increasingly being asked to consider how well the IT is being managed (COBIT, 2007). Organisations must, therefore, ensure that they have in place security controls to ensure the confidentiality,

integrity and availability of their information (ISO/IEC 27002, 2005). The executive management, which is ultimately accountable for an organisation's success is, therefore, responsible for the protection of the organisation's information (De Haes and Van Grembergen, 2008).

This chapter emphasises that it is imperative that the executive management of an organisation is committed to and responsible for information security within the organisation. This commitment entails complying with government's regulatory requirements while, at the same time, ensuring good Corporate Governance within their organisations. The next sections discuss Corporate Governance and IT Governance.

2.3 Corporate Governance

Corporate Governance is increasingly becoming a major requirement of good organisational management following the collapse of giant organisations such as Worldcom, Enron and Tyco (Doughty and Grieco, 2005). The failures of these organisations were the result of financial mismanagement and the poor governance exercised by the executive boards. In response to these governance failures, governments worldwide have formulated new laws and regulations aimed at protecting both investors and shareholders. As a result, it has become mandatory for executive management teams to adopt a more rigorous mechanism in terms of which to govern their organisations (King III Report, 2009).

The most noteworthy laws include the Sarbanes-Oxley and Graham-Leach-Bliley Acts. Section 404 of Sarbanes-Oxley, which focuses on internal controls, requires that systems storing or processing corporate financial information must include appropriate controls in order to protect such information (Sarbanes-Oxley, 2002). The Boards of directors are responsible for ensuring compliance with the requirements of these laws and regulations. This is not surprising in view of the fact that the executive team members are primarily responsible for the management of the organisation and for the strategic decisions in terms of which the organisation should operate.

The King III Report (2009) clearly stipulates that it is the duty of the executive directors to discharge their legal duties which are grouped into the following categories: the duty of care, skill and diligence, and the fiduciary duties. The report goes further by stating that "Corporate Governance mainly involves the establishment of structures and processes, with appropriate checks and balances that enable directors to discharge their legal responsibilities, and oversee compliance with legislation" (King III Report, 2009, p. 14).

2.3.1 Defining Corporate Governance

The IT Governance Institute (2005, p. 23) defines Corporate Governance as the "set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the enterprise's resources are used responsibly." This definition focuses on the way in which the organisation is managed and emphasises the importance of its resources being used effectively.

There is a growing number of prominent sources that may aid and guide executive management to ensure effective Corporate Governance in their organisations. These include the Organisation for Economic Co-operation and Development (OECD) Principles of Corporate Governance which state that "the Principles are intended to assist OECD and non-OECD governments in their efforts to evaluate and improve the legal, institutional and regulatory framework for Corporate Governance and to provide guidance and suggestions for stock exchanges, investors, corporations, and other parties that have a role in the process of developing good Corporate Governance" (OECD, 2004, p. 53).

For South African organisations, one of most important guidelines on what constitutes good Corporate Governance is the King Report which was issued by the South African Institute of Directors. The King Report II emphasises the accountability and responsibility of the board of directors in order to ensure the good Corporate Governance of their organisations. The report states that: "The board is the focal point of the Corporate Governance system. It is ultimately accountable and responsible for the performance and affairs of the company. Delegating authority to board committees or management does not, in any way, mitigate or dissipate the discharge by the board and its directors of their duties and responsibilities."

The third King Report on Corporate Governance was released in September 2009 and came into effect on 1 March 2010. The King Report III applies to all corporate entities, regardless of size and whether or not they are listed. King III does not provide a specific set of rules to organisations but it is a "principle-based document" (Temkin, 2009; Steenkamp, 2009). The King III Report is an extension of King I and King II which focused primarily on compliance governance practices. King III Report (2009) adopted the principle known as "apply or explain" which conveys the King Committee's intent to guide directors in deciding on the best practices to achieve the objectives of the Corporate Governance principles and to further explain how the principles and

recommendations should be applied. However, unlike its predecessors, King Report III addresses IT Governance.

2.4 Information Technology Governance

Despite the numerous discussions on Information Technology Governance (IT Governance), a variety of definitions of IT Governance have been suggested and from multiple perspectives (Simonsson and Ekstedt, 2006). According to Van Grembergen (2007, p. 23), "IT Governance is the organisational capacity exercised by the board, executive management and IT management to control the formulation and implementation of IT strategy and, in this way, ensure the fusion of business and IT." This definition indicates that an organisation's business objectives should be correlated with its IT objectives.

A more comprehensive definition of IT Governance is suggested by both King III (2009, p. 42) and Hardy (2006), namely, that IT Governance includes: "(i) understanding the risks surrounding IT, (ii) managing those risks through IT security and other controls, (iii) the strategic alignment of business and IT (ensuring that IT supports the business goals and direction) and (iv) the management of IT resources." This definition is more relevant to this research project than other definitions because it emphasises the management of the risks surrounding IT through the implementation of IT security controls – the core objective of information security management. The fact that security policies are one of the main security controls that should be used to mitigate the risks related to an organisation's information will be discussed in detail later in the study.

Bowen, Cheung, and Rohde (2007, p. 53) emphasise that organisations which have effective IT Governance processes in place experience the following benefits:

- "The reputation of the organisation is improved;
- Trust is built within the organisational as well externally;
- Risks in general are dismissed (and specifically the risk of financial damage and legal action due to an IT malfunction or malicious attack on the IT system); and
- The strategic alignment of IT with business goals and processes is achieved, leading to a competitive advantage (through decreased costs, increased costs, increased customer satisfaction and the ability to respond to business opportunities and challenges faster) which, ultimately, leads to an increase in revenue."

In view of the importance of IT Governance, it is obvious that IT Governance requires sound management involvement on the part of the top executive management. The next section will discuss the way in which executive management may ensure good Corporate Governance of IT.

2.4.1 Corporate Governance and IT Governance

The King III Report identified seven principles to which the board of executive management should adhere for the purposes of IT Governance. These are quoted directly from King III Report (2009, p. 56) below:

1. "The board should be responsible for IT Governance;
2. IT is aligned with the performance and sustainability objectives of the company;
3. The board should delegate to management the responsibility for the implementation of an IT Governance framework;
4. The board should monitor and evaluate significant IT investments and expenditure;
5. IT should form an integral part of the company's risk management;
6. The board should ensure that information assets are managed effectively;
7. A risk committee and audit committee should assist the board in carrying out its IT responsibilities".

These seven principles illustrate clearly that it is the responsibility of the executive management team to ensure good IT Governance.

The ISO/IEC 38500 international standard includes the guidelines for IT Corporate Governance. The objective of the ISO/IEC 38500 standard is to provide a framework of principles for directors to use when evaluating, directing and monitoring the use of IT within their organisations (ISO/IEC 38500, 2008). ISO/IEC 38500 recommends that directors should govern IT through the following three main tasks:

- "Evaluate the current and future use of IT;
- Direct preparation and implementation of plans and policies to ensure that use of IT meets business objectives;
- Monitor conformance to policies, and performance against the plans."

Figure 2.1 presents the model of IT Governance as proposed by ISO/IEC 38500 (2008).

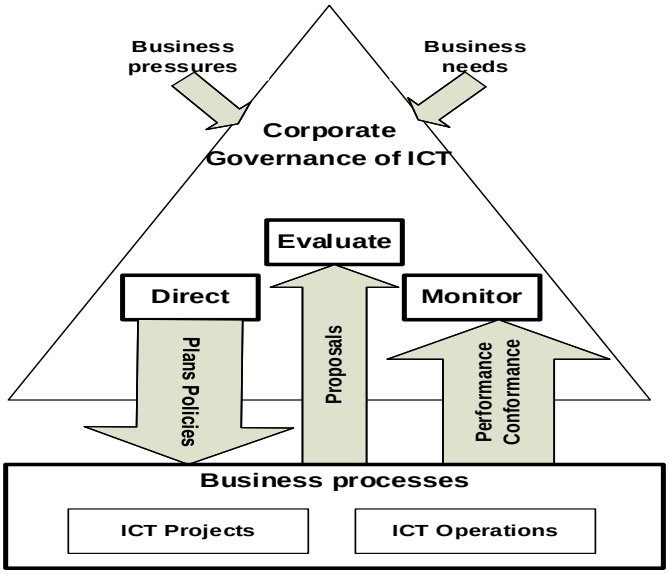


Figure 2.1: Model for Corporate Governance of IT (ISO/IEC 38500, 2008)

The three main tasks involved in governing IT, namely, direct, evaluate and monitor, are briefly discussed below:

Direct

The task of directing involves guiding, motivating and supervising personnel in such a way that the organisation's objectives, goals and plans are achieved successfully (Posthumus, Von Solms, and King, 2010). The King Report III (2009) clearly states that it is the responsibility of the board to provide strategic direction or guidance as regards the way in which the organisation should operate. In order to do this, there should be in place an effective communication plan between the executive managers and their subordinates to ensure that the organisational objectives and goals are clearly understood from the highest level management down to the lowest level management.

Von Solms, Thomson, and Maninjwa (2011, p. 4) state that "directing refers to the process of stating what is to be expected or accomplished, usually documented in the form of policies." In this research project it is argued that, in order to give direction effectively, executive managers should rely heavily on the establishment of policies which should be communicated to their subordinates. ISO/IEC 38500 (2008) recommends that executive managers should assign the responsibility for and direct the preparation and implementation of plans and policies to ensure that the use of IT meets the business

objectives. The policies should establish sound behaviour as regards the use of IT (ISO/IEC 38500, 2008).

Evaluate

Executive managers should examine and make judgments on the current and future use of IT, including strategies, proposals and supply arrangements (whether internal, external, or both) (ISO/IEC 38500, 2008). In terms of information policy implementation, Von Solms et al. (2011) refer to "evaluate" as the process which management uses in order to determine whether the individual policies have been complied with.

Monitor

Executive managers should monitor the performance of IT through appropriate measurement systems and ensure that such performance is in accordance with plans, particularly as regards the business objectives (ISO/IEC 38500, 2008). In the introduction to this chapter, it was pointed out that it is essential that organisations have in place an effective information security management plan in order to protect their information asset. This may be achieved through the establishment of Information Security Governance.

2.5 Information Security Governance

Information Security Governance is the term which is used to describe how information security is addressed as a component of the Corporate Governance responsibilities of an organisation. Information Security Governance involves all the stakeholders in an organisation, from the chairman of the board to the youngest departmental secretary (Von Solms and Von Solms, 2009).

According to Von Solms (2005, p. 3), "Information Security Governance consists of the management commitment and leadership, organisational structures, user awareness and commitment, policies, procedures, processes, technologies and compliance enforcement mechanisms, all working together to ensure that the **Confidentiality**, **Integrity** and **Availability** (CIA) of the company's electronic assets (data, information, software, hardware, people, etc.) are maintained at all times."

The objective of **confidentiality** is to ensure that sensitive information and data are protected from unauthorised disclosure (ISO/IEC 27002, 2013; Gerber et al., 2001). This, in turn, means that sensitive information must be kept secret and that access to such information is given only to entities that have permission to use it. Currently,

organisations face serious consequences if confidential information is leaked and appears in the media and social networking.

Ensuring the i**ntegrity** of information resources involves maintaining the correctness and comprehensiveness of that information (Humphreys, 1998; Björck, 2008). The purpose of integrity is to ensure that information remains in its original form and that no tampering or alteration takes place (Kritzinger and Von Solms, 2006). The integrity of information is important because information plays a major role in the decision making process (Ritchie and Brindley, 2001; Posthumus and Von Solms, 2006). Within the healthcare environment, for example, if health information is not accurate or complete, this may result in unwanted situations which may even lead to death or individuals being treated with inefficient medications.

The **availability** of information guarantees that information resources are accessible for use by authorised users at the time they wish to use the information (ISO/IEC 27002, 2005). According to Gerber and Von Solms (2001), ensuring the availability of information is crucial because, without timely information, an organisation would be incapable of continuing its normal operations.

In addition to protecting the confidentiality, integrity and availability of information, the IT Governance Institute (2005, p. 7) confirms that Information Security Governance adds significant benefits value to an organisation by:

- "Improving trust in customer relationships;
- Protecting the organisation's reputation;
- Decreasing likelihood of violations of privacy;
- Providing greater confidence when interacting with trading partners;
- Enabling new and better ways to process electronic transactions;
- Reducing operational costs by providing predictable outcomes – mitigating risk factors that may interrupt the process."

As discussed in Chapter 1, the weakest link in an organisation's information security is the insiders who, either intentionally or unintentionally, constitute the security threats. Threats to information security include multiple dimensions, including internal vs. external, human vs. non-human, and accidental vs. intentional.

2.5.1 Insider threats to information security

According to Duncan, Creese, and Goldsmith (2012, p. 26), "insider attacks are the realisation of the risk to companies, their data, their business partners and their long-term future caused by insiders becoming malicious and acting upon it." The literature review indicates that both intentional and unintentional insider threats have been regarded as one of the top ranked threats to information security over the past decade (Richardson, 2009). Duncan et al. (2012) maintain that there are two types of insider threats, namely, authorised insiders who have access to the network and those who are able to gain access opportunistically, for example, former staff members with access, auxiliary staff, for example cleaners, and external actors, for example building contractors.

Colwill (2009) discusses that an insider threats have the potential to cause more damage to the organisation as compared to outsider threats because such insiders have legitimate and often privileged access to facilities and information, they have knowledge of the organisation and its processes and they know the location of critical or valuable assets. Insiders will know how, when and where to attack and how to cover their tracks (Colwill, 2009).

The literature points out that, in many cases, insider threats are handled internally and no legal actions are taken because organisations are concerned with the negative publicity and reputation damage they may suffer. As depicted in Table 2.1, the CyberCrimeSurvey (2014) cited the major reasons why cybercrimes were not referred for legal actions.

Table 2.1: Reasons why cybercrimes are not referred for legal action (CyberCrimeSurvey, 2014)

Reasons CyberCrimes were not referred for legal action	2013	2012	2011
Damage level insufficient to warrant prosecution	34%	36%	40%
Lack of evidence/not enough information to prosecute	36%	36%	40%
Could not identify the individual/ individuals responsible for committing the eCrime	37%	32%	37%
Concerns about negative publicity	12%	9%	14%
Concerns about liability	8%	7%	9%
Concerns that competitors would use incident to their advantage	7%	6%	7%
Prior negative response from law enforcement	8%	5%	6%
Unaware that we could report these crimes	6%	5%	4%
Suggested incident was national security related	3%	4%	4%
Other	8%	12%	11%
Don't know	21%	28%	20%

The next section discusses the relationship between Corporate Governance, IT Governance and Information Security Governance.

2.6 Relationship between Corporate Governance and Information Security Governance

Corporate Governance includes all aspects of the governance of the entire organisation and, thus, the executive managers are responsible for both IT Governance and Information Security Governance. In view of the fact that information is the lifeblood of any organisation, it is crucial that information security processes and activities be integrated into the Corporate Governance structure. "Information Security is often treated solely as a technology issue, when it should also be treated as a governance issue" (Williams, 2007, p. 5).

"Information Security Governance is a subset of Corporate Governance that provides strategic direction, ensures that objectives are achieved, manages risks appropriately, uses organisational resources responsibly, and monitors the success or failure of the enterprise security program" (Von Solms and Von Solms, 2009, p. 7). Figure 2.2 illustrates the relationship between Corporate Governance, IT Governance and Information Security Governance (Von Solms and Von Solms, 2009).

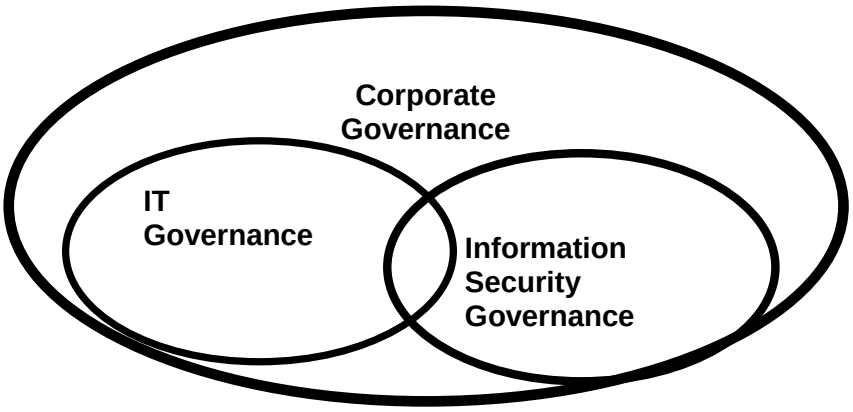


Figure 2.2: Information Security Governance positioned (Von Solms and Von Solms, 2009)

According to Information Security Governance (2004), the most effective way in which to strengthen information security is to treat it as a Corporate Governance issue that requires the attention of corporate boards and CEOs. King III (2009) highlights that,

without top management support, those responsible for applying information security experience difficulties in implementing an effective information security plan.

Research has found that directors tend to delegate security matters to the IT department because IT is perceived as a technical issue (Lohmeyer, Mccrory, and Pogreb, 2002). However, many theorists argue that information security is an extremely important issue within the organisation and that it should remain within the sphere of the directors (McFadzean, Ezingeard, and Birchall, 2008).

Johnston and Hale (2009) found that when information security is addressed at the corporate level as part of the organisation planning process, employees are more accountable for the security of their assets than would otherwise have been the case and they view security not as a barrier to success, but as an enabler.

2.6.1 Information security as a board issue

Based on the six factors discussed below, McFadzean et al. (2008) argue that information security is an extremely sensitive issue and that should remain within the sphere of influence of executive management. These factors include:

Authority

Kankanhalli, Teo, Tan, and Wei (2003) and McFadzean et al. (2008) point out that organisations require the support of top executives for the successful implementation of an information security plan. According to Lohmeyer et al. (2002) and McFadzean et al. (2008), executive management have the authority to the dimensions necessary for the implementation of an information security plan, including human issues, legal factors, policy-making, communication, and measuring and monitoring systems.

Leadership

McFadzean et al. (2008) recommend that the information security should be integrated into the organisation's corporate culture. It is essential that employees and the organisation's stakeholders practise sound information security behaviours in their daily activities.

Corporate Governance responsibilities

One of the responsibilities of senior management is risk management (King Report III, 2008). According to ITGI (2005, p. 9), "risk management requires risk awareness by

senior corporate officers, a clear understanding of the enterprise's appetite for risk, understanding of compliance requirements, transparency about the significant risk to the enterprise, and embedding of risk management responsibilities in the organisation."

Vision

The executive management is in charge of the business activities of the entire organisation and, therefore, it has a holistic view of the organisations' operations. McFadzean et al. (2008) emphasise that management should be involved in the assessment of the organisation's information value and that management should offer recommendation on the information which merits the more stringent protection measures.

Good management practice

Von Solms (2001) argues that it is the responsibility of the board of directors to guarantee that the organisation's staff, technology and systems are adequate and appropriate to ensure that the company remains competitive. If the organisation is to remain competitive, it is essential that the organisation ensures that there are mechanisms in place to protect its information systems (McFadzean et al., 2008).

IT and Information Security Governance

Korac-Kakabadse and Kakabadse (2001) and McFadzean et al. (2008) state that information security is part of IT Governance and, therefore, the board should be engaged in discussions about the assessment of information security related risks as the latter forms part of good IT Governance.

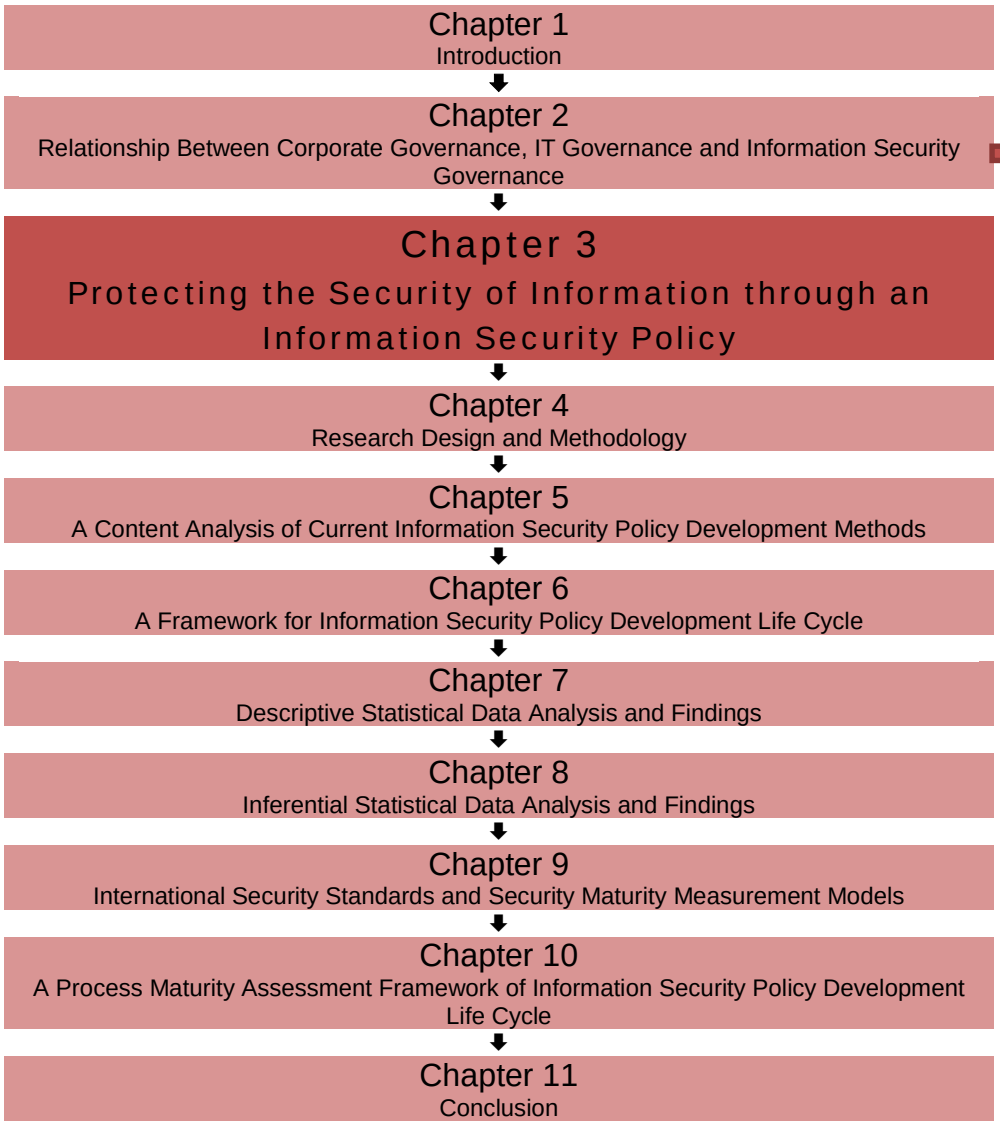
2.7 Conclusion

This chapter highlighted that organisations are extremely dependent on IT as IT supports the day-to-day transactions and many of the critical business functions of an organisation. Unfortunately this dependency on IT has resulted in an increase in the potential threats to an organisation's information (Edwards, 2011). It is, thus, essential that organisations have in place controls to protect their information assets. Furthermore, in the current integrated, regulated and litigated environment, it is important that organisations are able to provide assurance to their customers, stakeholders, regulators and the courts that the executive management teams have exercised due diligence in ensuring the security of information. This may be achieved through sound leadership on the part of the executive team which is, ultimately, both responsible and accountable for the good governance of

the organisation. This chapter also highlights that it is essential that organisations protect their information through effective Information Security Governance. Information Security Governance is a component of IT Governance which is, in turn, a component of Corporate Governance.

This study argues that effective information security policies constitute the main controls with which to mitigate the security threats caused by insiders. Chapter 3 focuses on the importance of information security policies and on the challenges related to developing such policies.

Chapter 3: Protecting the Security of Information through an Information Security Policy



CHAPTER 3:
Protecting the Security of Information through an Information Security Policy

- **3.1. Introduction**
- **3.2. Types of policies**
- **3.3. Importance of having an effective information security policy**
- **3.4. Challenges in developing and implementing an effective information security policy**
- **3.5. Existing theories related to information security policy compliance**
- **3.6. Conclusion**

3.1 Introduction

As discussed in Chapter 2, organisations depend on information systems and technologies if they wish to survive and thrive in an increasingly competitive environment. It is, thus, important that organisations have in place security measures that aim to protect the confidentiality, integrity and availability of the information embedded in these information systems. This study states that well-planned and effective information security policies constitute the major security controls to ensure the security of an organisation's information.

This chapter aims to discuss the importance of an information security policy. In addition, it highlights the challenges involved in the development and implementation of an effective information security policy. The chapter also discusses the dangers of conducting business in the information age without such a policy in place. Finally, the chapter explores existing theories that are linked to information security policy compliance.

3.2 Types of policy

The literature lists numerous types of policy. Von Solms et al. (2011) recommend a hierarchical structure for an ISPA which encompasses three general types of security policies, namely, **strategic level policies, tactical level policies and operational level policies**. This structure is depicted in Figure 3.1 with a direct arrow going all the way from the strategic level to the operational level.

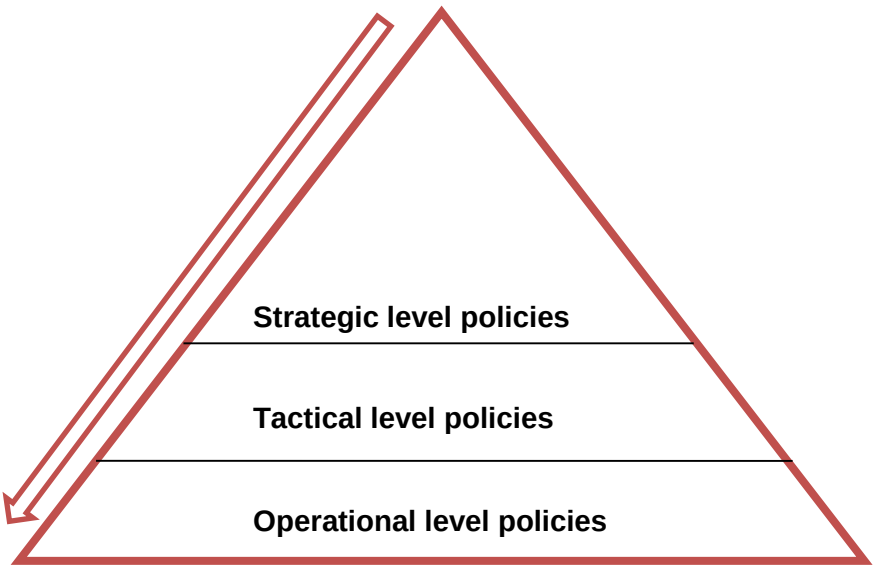


Figure 3.1: A comprehensive Information Security Policy Architecture (Von Solms et al., 2011)

The following section discusses the three types of policies.

3.2.1 Strategic level policies

Executive management highlights how critical the information assets are throughout the organisation through the implementation of a set of directives detailing the objectives aimed at protecting such information assets (Von Solms et al., 2011). Diver (2007) claims that these directives are dealt by managers in order to gain a sense of the company's overall security policy philosophy. According to Bayuk (2009, p. 1), strategic level policies are "a set of management mandates with respect to information security, these mandates provide the marching orders for the security professional."

Von Solms et al. (2011, p. 3) refer to such a policy as a "Corporate Information Security Policy (CISP)", "Enterprise Information Security Policy (EISP)", "information security programme policy", "general security policy", "IT security policy" and "high-level information security policy." Whitman and Mattord (2008, p. 113) refer to these policies as "information security policy"; while the National Computer Board Mauritius (2011, p. 5) terms these policies "governing policy." For the sake of consistency, these types of policies will be referred in this study as high level security policies because they are implemented at the top management level.

3.2.2 Tactical level policies

At the tactical level the high level information security policies emanating from the strategic level are transformed into organisational standards and guidelines that highlight detailed instructions as regards the use of the organisation's processes, technologies, or systems (Whitman and Mattord, 2008, p. 111; Von Solms et al., 2011).

The policies at the tactical level are also known as technical policy (Mauritian Computer Emergency Response Team, 2011), tactical level policy or issue specific policy (Von Solms et al., 2011). The Mauritian Computer Emergency Response Team (2011, p. 6) states that "technical policies describe what must be done, not how to do it". This is reserved for procedural documents which are the next detail level down from governing and technical policy. In terms of detail level, technical policy should address the "what" (in more detail), "who", "when" and "where" in terms of information security policy". In this study, these policies will be referred as detailed security policy because they provide detailed guidelines concerning the implementation of the high level security policies.

3.2.3 Operational level policies

At the operational level the detailed information security policies are supported by lower level security policies which are also known as procedures (Von Solms et al., 2011). The procedures contain the step-by-step, detailed instructions on how to meet the requirements of an information security policy (Diver, 2007). The Mauritian Computer Emergency Response Team (2011) states that procedures are the same as the manuals that guide employees in protecting an organisation's information security policy. The security policies at operational level are referred as system-specific policy (Whitman and Mattord, 2008, p. 97), low-level policy (Verma, 2000), application specific policy (Peltier and Blackley, 2005) and procedures (Mauritian Computer Emergency Response Team, 2011). For the purposes of this research project, these policies will be referred as lower level security policies.

3.2.4 Information Security Policy Architecture

Von Solms et al. (2011) maintain that an organisation's information security policies, namely, the strategic and tactical level policies, are normally organised in an Information Security Policy Architecture (ISPA). Bacik (2008, p. 11) defines ISPA as "a set of documents, comprising policies, guidelines, standards, procedures, and memorandums that collectively contributes to the protection of organisational assets." Whitman and Mattord (2008, p. 124) state that: "Information Security Policy Architecture should ideally tie together all information security related policies, from the Corporate Information Security Policy (CISP) right down to the lowest level technical or operational information security policies." This study is intended to investigate the processes that an information security policy should go through in its life time. Accordingly, the ISPA is a type of policy which is suitable for this study as it combines the other three types of policies.

3.3 Importance of an effective information security policy

The literature agrees that effective information security is based on a sound information security policy (Parker, 1998; Warman, 1992, McFadzean et al., 2008; Bayuk, 2009). Bayuk (2009) points out that an information security policy is the cornerstone of an information security programme while Hone and Eloff (2002) and Von Solms and Von Solms (2005) claim that the most important mechanism for protecting corporate information is the formulation and application of an effective information security policy.

Kadam (2007) views information security policies as part of the step which follows the risk assessment and in terms of which policies and control strategies are developed in order to mitigate the risks. ISO/IEC 27002 (2013) refers to an information security policy as a document that guides the management for information security in order to meet the business objectives and regulations requirements.

According to the National Computer Board Mauritius (2011, p. 6), an information security policy should fulfil the following purposes:

- "Protect people and information;
- Set the rules for expected behaviour by users in organisation;
- Authorise security personnel to monitor and investigate security;
- Define and authorise the consequences of security policy violation;
- Define the company consensus baseline position on security;
- Help reduce risks;
- Help track compliance with regulations."

Maynard et al. (2011) highlight that information security policies are crucial documents in ensuring compliance with the requirements of an organisation's regulations. According to Etsebeth (2006), an information security policy is a document that should provide both directors and top management with concrete evidence to present in court that they have fulfilled their responsibility of due care and diligence.

As discussed above, there is no doubt that an information security policy contributes significantly to the well-being of an organisation as regards the protection of its information security and its compliance with the regulation requirements of government. However, the processes of developing, implementing and adopting an effective information security policy are difficult at best.

3.4 Challenges in the development and implementation of an effective information security policy

InformationShield (2010) points out that the information security policy development is driven by new regulatory requirements; external threats such as hackers and crackers; the increased use of new communication technology such as wireless using Voice Over the Internet Protocol (VOIP); insiders' behavioural use of internet and, new technology deployment encryption and anti-virus software issues. The development of security

policy takes into account all these requirements. Figure 3.2 depicts these security policy drivers diagrammatically:

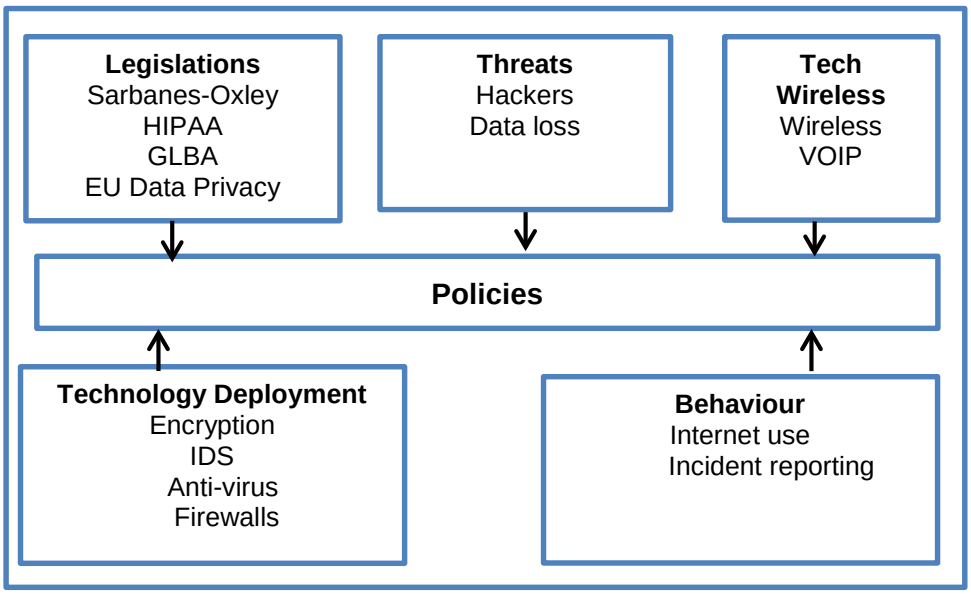


Figure 3.2: Security policy drivers (InformationShield, 2010)

In addition to the different security policy drivers highlighted in Figure 3.2, the literature does not offer a comprehensive method for developing an information security policy.

3.4.1 Lack of guidance for the development and implementation of information security policy

The literature focuses on descriptions of the structure and the content of an information security policy but, in general, its fails to describe in detail the processes which are used to generate the output of an information security policy. In addition, the literature presents numerous studies which are related to information security policy compliance, for example, studies conducted by Bulgurcu et al. (2010), Herath and Rao (2009), Johnston and Warkentin (2010), Myyry et al. (2009), Siponen and Vance (2010) and Warkentin et al. (2011). These studies were driven by the motivation to understand the factors which either enable or inhibit compliance with information security policy. As highlighted in the next section, the existing literature on information security policy development details mechanisms for developing security policies.

In view of the lack of a model or framework that clearly depicts the step-by-step process involved in developing and implementing information security policies, security policy developers experience difficulties in constructing security policies that meet the business

requirements of their organisations. According to McKenna (2010, p. 5), "unfortunately, many IT security people do not understand business IT alignment, so they end up writing these huge security policies that are all about protecting everything." The next section discusses the current methods/approaches used in developing information security policies.

3.4.2 A gap in the current security policy development and implementation methods

A review of relevant literature reveals certain information security policy development and implementation methods which organisations may use for the development of a custom security policy. Table 3.1 presents an informal comparison of a few examples of these methods.

Table 3.1: Comparison of information security policy development methods

Tech4Law (2009)	Laura (2010)	Kadam (2007)	Avolio et al. (2007)	Yayla, (2011)
1.Research policy content	1.Identify legal requirements	1.Identify the threats to the business processes	1.Create the policy	1.Write policies
2.Draft policy	2.Develop information security policy	2. Identify the vulnerabilities of the business processes	2.Determine penalties for contravening the policy	2.Conduct security policy training
3.Issue policy to staff	3.Document an information security policy	3.Formulate individual policies which address each vulnerability	3.Enforce the policy	3.Security policy awareness
4.Monitor and maintain policy	4.Review security policy with management, executives and stakeholders	4.Write information security policy	4.Review policy using policy request changes.	4.Enforce security policies through deterrence measures
5.Obtain management approval		5.Write procedures and guidelines		
		6.Implement security policy at both the top and the operational levels		

As depicted in Table 3.1, the existing literature on information security policy development and implementation methods provide basic steps in the development of a security policy document. The security policy development process that is probably the process with the most focus on policy creation is the process suggested by Kadam (2007). This process

addresses risk assessment, security policy construction and the implementation of the policy.

The comparison also reveals certain similarities in terms of which the writers are in agreement on the same steps. However, the comparison also reveals the gaps in terms of which a particular writer has not mentioned a step that the others consider as important. For example, Tech4Law (2009), Avolio et al. (2007) and Yayla (2011) do not mention any actions required as part of the risk assessment stages while Kadam (2007) considers risk assessment as the main step to be conducted before attempting any steps in policy construction. In addition to the challenges already mentioned, it would appear that the major problem is the maturity assessment of the security policy development processes.

3.4.3 Lack of guidance for assessing the maturity of the information security policy development and implementation processes

There seems to be no evidence of a comprehensive and integrated assessment tool with which to assess the processes involved in developing and implementing an information security policy. Concerning the information security policy, the literature focuses on the assessment of the information security policy in terms of the content and structure of information security.

Grobler and Von Solms (2008) proposed a model in terms of which to assess the information security status of an organisation and which contains special reference to the policy dimension. This six-step proposed model includes assessment checklists to evaluate the completeness of the policy set, the format of documented policies, whether adequate supporting documentation exists and whether a policy management system exists.

Maynard and Ruighaver (2006) proposed a framework for assessing the quality of the information security policy. Their framework includes a number of factors that should be taken into account in order to assess the quality of the information security policy within an organisation. These factors include functionality, maintainability, portability, efficiency, reliability and usability.

Diver (2007) emphasises that organisations should first investigate the maturity of the policy development process that is currently in place before embarking on developing a security policy. According to Diver (2007, p. 1), “a company which currently has no

information security policy or only a very basic one may initially use a different strategy to a company which already has a substantial policy framework in place, but wants to tighten it up and start to use policy for more complex purposes such as to track compliance with legislation". Chapters 9 and 10 in this research project will focus on the maturity assessment of the information security policy development life cycle.

3.4.4 Regulatory requirements for information security policies

With the increasing number of regulatory requirements, it is important that organisations have mechanisms in place to ensure compliance with such regulatory requirements. In an organisation, if an employee either intentionally or unintentionally makes a mistake that is in breach of the regulatory requirements, the organisation will be legally liable for the mistake made by the employee (Etsebeg, 2009). It is, thus, essential that organisations seek legal advice to ensure that their policies are legally binding (Maynard et al., 2011) and that employees who violate such policies will be legally liable for their behaviour.

The InformationShield (2010) contains a summary of examples of laws that require that management ensure that information security policies are implemented in their organisations as shown in Table 3.2.

Table 3.2: Regulatory requirements for information security policies (InformationShield, 2010)

Regulation / Framework	Industry/Country	Policy requirement
HIPAA (Health Insurance Portability and Accountability Act of 1996) Security Final Rule	Healthcare (U.S)	Policies and Procedures 164.316 (a) (R)" Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart".
Sarbanes-Oxley Act, Section 404 - based on COBIT: Control Objectives, Section 6: Communicate Management aims and directions.	All Publicly Traded Companies (U.S)	6.2 Management's Responsibility for Policies: "Management should assume full responsibility for formulating, developing, documenting, promulgating and controlling policies covering general aims and directives."
New Basel Capital Accord (Basel II)- Quantitative Standards, Section 606	Banking (International)	Gramm-Leach-Bliley Act (GLBA) Title V - Section 501: "Interagency Guidelines Establishing Standards for Safeguarding Customer Information".

Regulation / Framework	Industry/Country	Policy requirement
FERC Cyber Security Standard CIP-003-1 Security Management Controls	Energy/Infrastructure (U.S.)	Requirement1: "The Responsible Entity shall create and maintain a cyber-security policy that addresses the requirements of this standard and the governance of the cyber security controls."
Federal Information Security Management Act (FISMA) NIST SP 800-26	Federal Government (U.S.)	"(a) The head of each [Federal] agency shall delegate to the agency Chief Information Officer ensuring that the agency effectively implements and maintains information security policies, procedures, and control techniques."
PIPEDA (Bill C6) - Personal Information Protection and Electronic Document Act	All Industries (Canada)	4.1 Principle 1 - Accountability "Organisations shall implement policies and practices to give effect to the principles". 4.8 Principle 8 - Openness "Organisations shall be open about their policies and practices with respect to the management of personal information."
EU Data Protection Directive	All Industries (European Union)	"Organisations must implement appropriate technical and organisational measures to protect personal data."

As shown in Table 3.2, governments are forcing organisations to have security policies in place in order protect the citizens' information. Another challenge is the cost required to accomplish necessary tasks of information security policy development.

3.4.5 The cost related to information security policy development

Lineman (2009) highlights the various activities and associated costs related to the review and development of information security policy as shown Table 3.3.

Table 3.3: The total cost of policy management (Lineman, 2009)

Activity	Effort per quarter	Cost
Review regulatory changes	8 hours	$ 800.00
Review new technologies	8 hours	$ 800.00
Review major incidents	4 hours	$ 400.00
Write new policies	12 hours	$ 1 200.00
Map to frameworks	4 hours	$ 400.00
Total cost	36 hours	$ 3 600.00

As shown in Table 3.3, it is essential that organisations ensure that they have sufficient money before embarking on the process of developing information security policies.

However, the decision as regards the allocation of the budget will depend on the results of the risk assessment and the risk appetite conducted by the organisation. This issue will be further discussed in Chapter 6.

3.4.6 Information security policy not linked to risk assessment

McKenna (2010) claims that the main problem related to information security policies development stems from the fact that the policies are often written prior to conducting the risk assessment. According to McKenna (2010, p. 6), "Security policy should be risk based, and always around where you are having issues." Information security policies that are risk based will be capable of nullifying the threats that were identified during the risk assessment. Thus, such security policies will provide proper direction for information security within organisations.

3.4.7 Issue of information security policy compliance, awareness and review

Hoffman (2008) argues that employees often do not comply with information security policy as a result of the lack of a communication and awareness mechanism being implemented in the organisation. According to Hoffman (2008, p. 3), “The majority of companies have security policies in place, but research reveals that employees often defy or ignore them. The reason? They likely don't even know their company has a security policy.”

Another problem related to the information security policy is the fact that it is often never reviewed. This, in turn, results in the neglect of legal responsibilities and outdated policies. Abdel-Aziz (2010) states that it is imperative that security policies are consistent with the regulatory requirements. Governments vote in new laws while other laws are amended and, thus, security policies must be reviewed to ensure consistency with the regulatory requirements. In addition, the review process should reflect the lessons learnt from recent incidents while also taking into account new threats that have emerged (Abdel-Aziz, 2010).

Another important issue is employees violating information security policies as a result of negligence and/or ignorance. The Data Breach Investigation Report (2012) conducted by the Verizon RISK Team revealed that, of the 855 incidents reported, 90% had involved insiders who had deliberately caused the malicious actions by not adhering to the organisations’ information security policies.

This study relies on existing theories related to information security policy compliance in order to understand the various rationales that explain why employees may choose either to comply with or decide to violate the requirements of the information security policy.

3.5 Existing theories related to information security policy compliance

There is agreement in the literature that the major threat to an organisation's information security involves careless insider employees who intentionally violate the organisation's information security policies (Bulgurcu and Cavusoglu, 2008; Hassandousset et al., 2011; Ifinedo, 2012). Various theories and approaches have been developed in order to address this concern – for example, General Deterrence Theory, Theory of Reasoned Action and Theory of Planned Behaviour. These theories are discussed in the following section in order to gain an understanding of the factors that result in employees either complying with or violating an organisation's information security policy.

3.5.1 Theory of Planned Behaviour

The Theory of Planned Behaviour (TPB) is an extension of the Theory of Reasoned Action (TRA) (Ajzen and Fishbein, 1980). The TRA was developed by Fishbein and Ajzen (1967) and it states that people's behavioural intentions are influenced by both attitude and subjective norms (Fishbein and Ajzen, 1975).

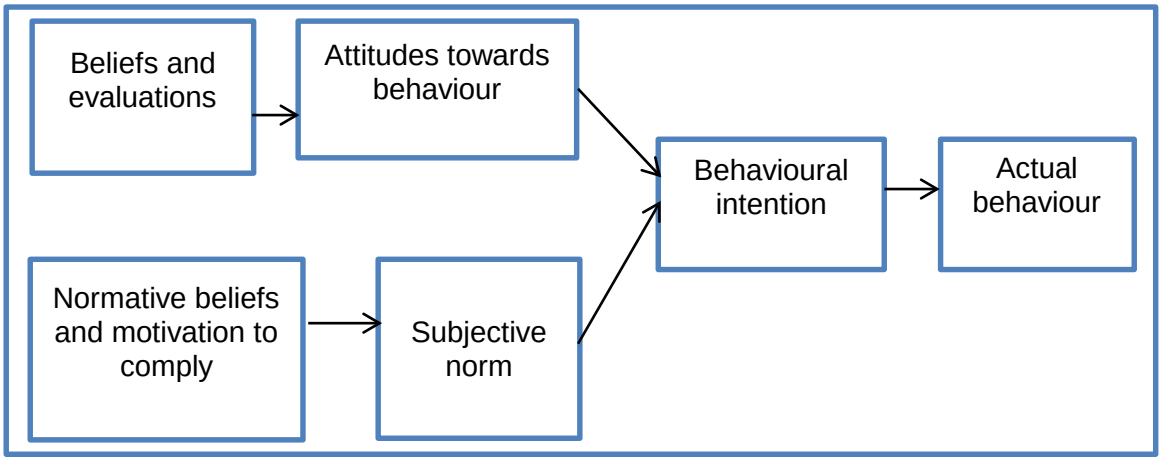


Figure 3.3: Theory of Reasoned Action (Fishbein and Ajzen, 1975)

The TPB adds perceived behaviour control to the TRA. The theory explains that the intention of an individual to perform a given behaviour is influenced by attitude, subjective

norms and perceived behavioural control (Fishbein and Ajzen, 1975). A graphical illustration of TPB is presented in Figure 3.4.

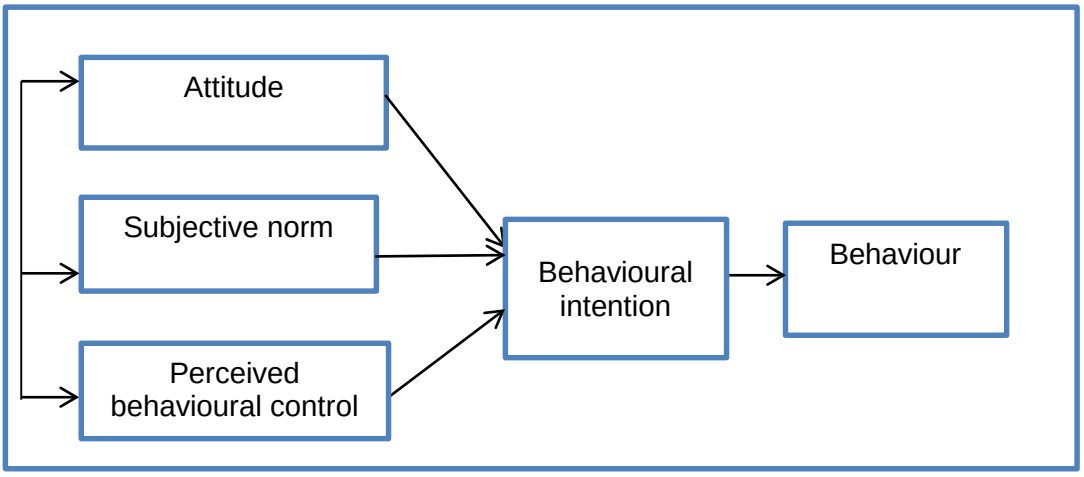


Figure 3.4: Theory of Planned Behaviour (Fishbein and Ajzen, 1975)

Attitude is defined by the person's positive or negative feelings towards carrying out a certain behaviour and it is determined by the person evaluating his/her beliefs regarding the consequences of performing the behaviour (Ajzen, 1991). Employees with positive beliefs about an organisation's information security policies are likely to comply with the requirements of such policies (Ngel et al., 2009; Herath and Rao, 2009; Bulgurcu et al., 2010; Ifinedo, 2012).

Subjective norms refer to a person's perception of what the people important to them would think about a given behaviour (Fishbein and Ajzen, 1967). Chan et al. (2005) state that employees tend to comply with information security policies if they realise that their colleagues, including peers, supervisors and managers, are complying with such security policy requirements.

Perceived behaviour, which is also termed self-efficacy control, was influenced by the work of Bandura (1991). Perceived behaviour refers to a person's perceived ease or difficulty as regards performing a certain behaviour (Ifinedo, 2012). Perceived behaviour is influenced by the availability of resources and opportunities (Ajzen, 1991). The study conducted by Ifinedo (2012) identified that self-efficacy has a positive effect on information security policy compliance. According to Lee and Larsen (2009, p. 3), "individuals are reticent to follow or adopt recommended responses if they perceive that a considerable amount of resources i.e. time, effort and money will be expected toward effort of such responses."

3.5.2 General Deterrence Theory

General Deterrence Theory (GDT) predicts that an increase in the severity of the punishment imposed on those who violate the rules of the organisation reduce the incidence of certain criminal acts (Blumstein et al., 1978). The objective of GDT is to increase prevention and deterrence in order to reduce unpunished abuse (Straub and Nance, 1990; Straub and Welke, 1998).

The literature clearly demonstrates that GDT has been used extensively in the information security field to help employees comply with information security requirements (Hoffer and Straub, 1989; Kankanhalli et al., 2003; Lee et al., 2004; D'Arcy, Hovav, and Galletta, 2009). Blumstein (1978) states that, if they are to be effective, the deterrence measures should put in place disciplinary actions that will be exercised when perpetrators are identified. According to Chen and Li (2014), employees will adhere to an organisation's recommendations if the punishment arising from misconduct is severe. In their study, Herath and Rao (2009) found that the severity of the penalty positively affects the intention to comply with organisational information security policies.

3.6 Conclusion

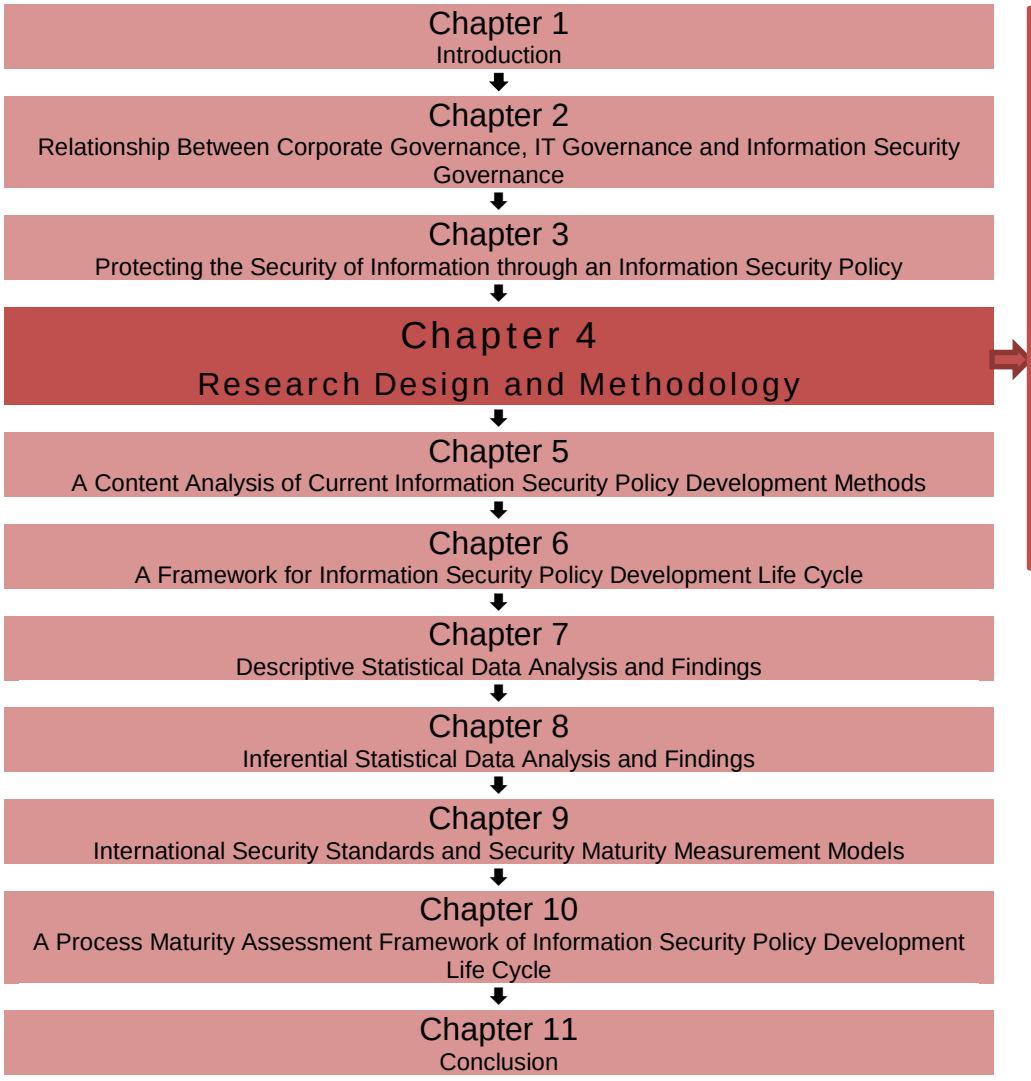
Threats to corporate information are constantly increasing at a time when businesses are relying more heavily upon information technology. It is, thus, evident that security managers must have in place proper controls to ensure the security of an organisation's information. This, in turn, entails an appropriate and effective information security management plan. Such a plan would not only enable employees to assume greater responsibility for information security than would otherwise have been the case, but it would also ensure that information security is not being compromised and that the information assets continue to be properly protected. In order to realise this objective, this study emphasises the role of sound information security policies as the main security control for effective information security management.

Nevertheless, the process of developing and implementing an effective information systems security policy is not a straightforward task. This process is driven by multiple factors such as new regulatory requirements, the complexities of new technologies and external and/or internal threats. The existing literature highlights certain information security policy development and implementation methods that an organisation may use to develop its information systems security policy. However, these methods do not include a comprehensive, integrated method that details step-by-step processes for developing

and implementing an information security policy. Accordingly, this study aims to find a solution to the problem of information security policy formulation, implementation and compliance in order to address the challenges that have been highlighted in this chapter.

Chapter 3 discussed the theoretical background to information security policy while Chapter 4 will focus on the research methodology that was used to realise the study's objective.

Chapter 4: Research Design and Methodology



CHAPTER 4:

Research Design and Methodology

4.1 Introduction

Upadhyaya (2013, p. 6) defines a research design as “the blueprint of the research that describes the methods used for the collection, measurement and analysis of data.” The main objective of this chapter is to describe the plan which was used in order to conduct this research project. The chapter highlights the philosophical stance underlying the study and discusses the research paradigm, research method, research strategy and data collection techniques used in the study. In particular, this chapter motivates the reason why a specific research methodology was chosen and also how this methodology made it possible to find solutions to the research problem. Saunders et al. (2009) are of the opinion that a research design comprises a research philosophy which may be as philosophical worldviews as well as the research approach, research strategy, research choices and research methods used. Figure 4.1 depicts the research design adopted for the purposes of this study.

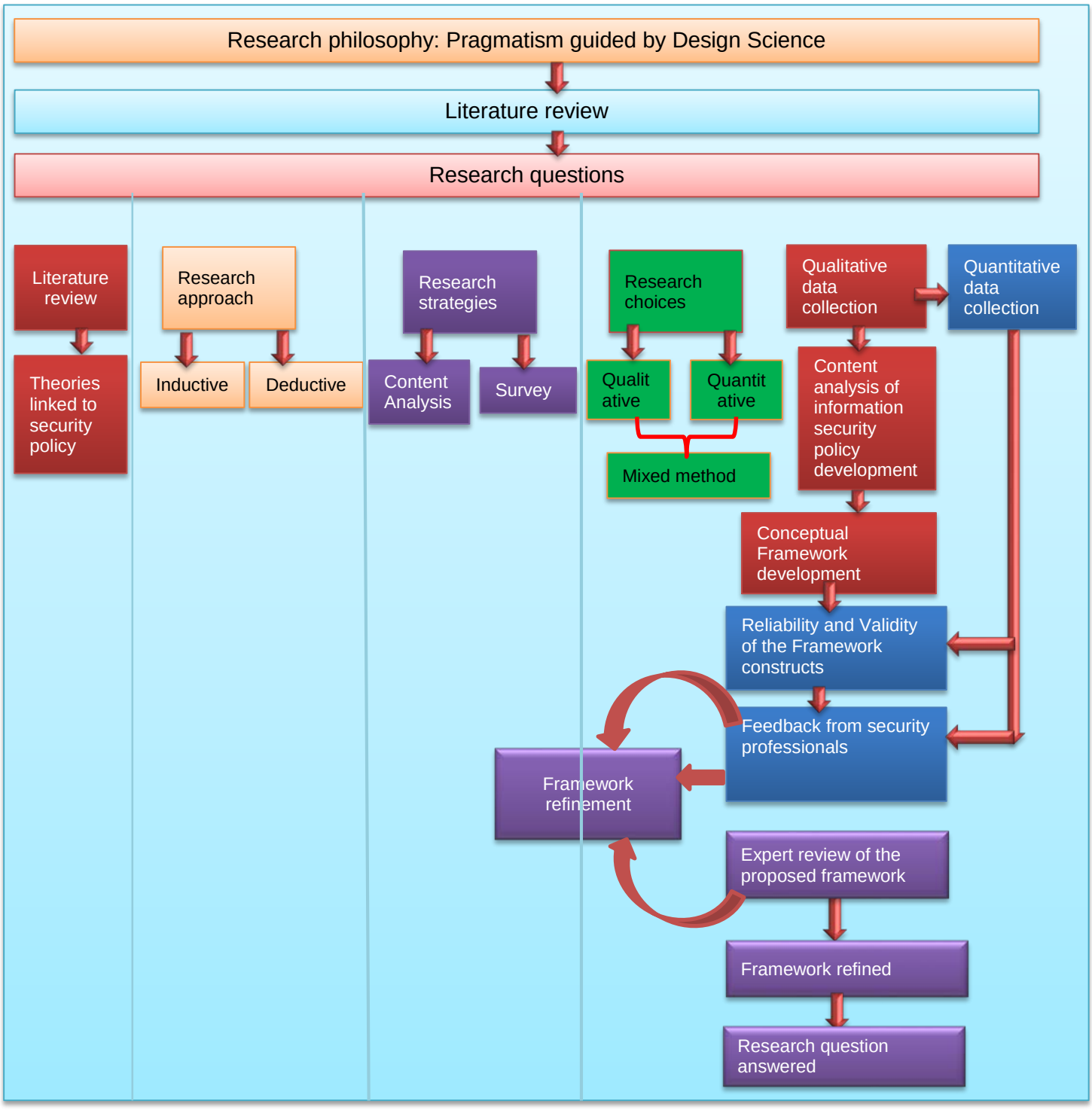


Figure 4.1: Research design

In any research project the researcher seeks to discover new knowledge or facts in a systematic or organised manner in order to make a contribution to the body of knowledge (Saunders et al., 2009). This task starts with a careful selection of a research topic, area of interest and research paradigm. Crossman (2003) maintains that understanding the research paradigm enables a researcher to decide on the overall research strategy to be

used in a particular research project by suggesting the most appropriate way in which to gather and interpret the evidence required to answer the research question.

The word paradigm originated from the Greek word *paradeigma* which means pattern (Webster Dictionary, 2001). The Webster Dictionary defines a paradigm as "an example or pattern: small, self-contained, simplified examples that we use to illustrate procedures, processes, and theoretical points." Khun (1962, p. 5) defines a paradigm “as the underlying assumptions and intellectual structure upon which research and development in a field of inquiry is based.” On the other hand, according to Bunniss and Kelly (2010, p. 7), “paradigms are sets of beliefs and practices, shared by communities of researchers, which regulate inquiry within disciplines and are characterised by *ontological, epistemological, axiology* and *methodological* differences in their approaches to conceptualising and conducting research, and in their contribution towards disciplinary knowledge construction.”

Saunders et al. (2009, p. 110) state that ontology is concerned with the nature of reality – What assumptions are being made about a reality?. Ontological philosophy aims at describing whether reality exists as a result of natural laws (objectivism) or whether it is constructed in the human mind and by experience (Krauss, 2005). On the other hand, epistemology is interested in what constitutes acceptable knowledge in a particular field of study (Saunders et al., 2009, p. 112). According to Easterby-Smith et al. (2008), epistemology refers to the philosophy of how knowledge of reality is derived, taking into account the sources of knowledge, methods of inquiry, and the limits of what can be known and what cannot be known. In addition, Saunders et al. (2009, p. 116) argue that a paradigm is characterised by an axiology which is, in turn, concerned with how values influence the perception and interpretation of realities.

According to Saunders et al. (2009, p. 119), there are philosophical assumptions on which research is based, namely, *positivism, realism, interpretivism and pragmatism*. Table 4.1 illustrates how these four research philosophies are related to ontology, epistemology, axiology and research methodology.

Table 4.1: Research philosophy summary (Saunders et al., 2009)

	Positivism	Realism	Interpretivism	Pragmatism
Ontology	Objective, independent of social actors	Objective, independent of human thoughts	Subjective, socially constructed	Multiple views, choose best representative view
Epistemology	Facts and observable data	Facts and observable data, but sensations also play a role	Social phenomena, situational	Integrate perspectives to interpret the data
Axiology	Value free researcher independence	Value laden and Researcher bias	Value bound and Researcher part of research	Values play a significant role
Methods	Quantitative	Quantitative	Qualitative	Mixed
Metaphor	Natural scientist	Realist	Social actor	Pragmatist

Each of the four paradigms presented in Table 4.1 is briefly discussed in the section below.

4.1.1 Positivism

The positivist paradigm, which is based on the philosophical ideas of the French philosopher, August Comte, defines knowledge in terms of empirically verifiable observation (Upadhyaya, 2013). According to Eriksson and Kovalainen (2008, p. 15), "positivism is based upon values of cause effect reasoning, focuses on falsifying or validating observable and experienced facts that may be empirically measured and generalised." Positivist researchers believe that knowledge is valid only within observable and measurable phenomena (Alwi, 2012). Saunders et al. (2009, p. 114) claim that one advantage of positivist approach is the credibility of the research results as the results are not influenced by the researcher's 'feelings'. "The assumption is that the researcher is independent of and neither affects nor is affected by the subject of the research" (Remenyi, Williams, Money and Swartz., 1998, p. 33).

4.1.2 Interpretivism

As regards the interpretivism paradigm, Saunders et al. (2007) state that the aim of the researcher is to understand and interpret the interactions, feelings and opinions of the research subjects in order to derive meanings in respect of the internal reality of subjective experience. Walsham (1995) further emphasises that interpretive researchers are attempting the difficult task of assessing other people's interpretations and filtering these interpretations through their own conceptual apparatus. During the data collection there is interaction between the researcher and the participant and this may, in turn,

influence the research findings Saunders et al. (2009, p. 115). Table 4.2 presents the main features of positivism and interpretivism (Collis and Hussey, 2009).

Table 4.2: Features of positivism and interpretivism (Collis and Hussey, 2009)

Positivism	Interpretivism
Uses large samples	Uses small samples
Have an artificial location	Have a natural location
Be concerned with hypotheses testing	Be concerned with generating theories
Produce precise, objective, quantitative data	Produce rich, subjective, qualitative data
Produce result with high reliability but low validity	Produce result with high validity but low reliability
Enables results to be generalised from the sample to population	Enables findings to be generalised from one setting to another similar setting
Use methodologies such as surveys, experimental studies and cross-sectional studies.	Use methodologies such as case studies, grounded theory and action research.

The next section discusses the realism paradigm.

4.1.3 Realism

Realism lies between the positivistic and interpretivist stances (Blaikie, 2010). The researchers believe that reality exists without human consciousness and independently of whether it has been proved or not (Saunders et al., 2007). The realism paradigm approaches natural sciences research and social sciences research in different ways (Chia, 2002). Realists assume an interpretivistic stance that reality is pre-interpreted and also a positivistic approach that scientific study is both empirical and objective (Chia, 2002).

4.1.4 Pragmatism

Pragmatism is a combination of philosophies that hold the view that it is possible to work with potential conflicting assumptions regarding the nature of reality as well as variations in the way in which knowledge may best be produced (Saunders et al., 2009, p. 109). Patton (2002, p. 71) motivates the use of pragmatism by stating: “My pragmatic stance aims to supersede one-sided paradigm allegiance by increasing the concrete and practical methodological options available to researchers and evaluators. Such pragmatism means judging the quality of a study by its intended purposes, available resources, procedures followed, and results obtained, all within a particular context and for a specific audience.” Pragmatism is used in mixed methods where the researcher needs to draw inferences from both the quantitative and the qualitative data in a single study (Cameron, 2011).

In addition to the four paradigms discussed above, Livari (2007) and Vaishnavi and Kuechler (2008) argue that the Design Science is emerging as a research paradigm with which to build IT artefacts. The next section discusses the Design Science paradigm.

4.1.5 Design Science as an emerging paradigm

Amrollahi et al. (2007) indicate that the term 'Design Science' was first coined in the 1960s in the architecture and engineering literature. Subsequently, Simon (1969) introduced it to Information Systems (IS). In 1990, Nunamaker and Chen (1990) introduced their methodology of IS research based on system development. Since then, Design Science "has become a popular approach for IS scholars and practitioners in solving real problems through developing and evaluating IT artefacts" (Amrollahi et al., 2007, p. 9). Table 4.3 describes examples of Design Science used as a paradigm (Amrollahi et al., 2014).

Table 4.3: Main theoretical works (Amrollahi et al., 2014)

Reference	Main contribution	Output focus	Design Science position
Livari (2003)	Defines "meta-artefacts" as way to enhance IS research	Research	Paradigm
Hevner et al. (2004)	DSR framework / seven guidelines for DSR / five evaluation methods	Artefact	Paradigm
Gregor and Jones (2007)	Eight components of design theories	Theory	Paradigm
Livari (2007)	Study of DSR in terms of ontology, epistemology, methodology and ethics	Research	Paradigm
Hevner (2007)	Complementary to DSR framework.	Artefact	Paradigm
Piffers et al. (2007)	Methodology for DSR with six steps	Artefact	Method
Kuechler and Vaishnavi (2008)	General design cycle of DSR	Theory	Paradigm
Pries-Heje and Baskelville (2008)	Set of constructs and methods named design theory nexus for addressing ill-structured or wicked problems	Artefact	Method
Kuechler and Vaishnavi (2012)	Design-relevant explanatory / predictive theory for theory development	Theory	Paradigm

Hevner et al. (2004) argue that IT artefacts design and evaluation have an impact on the environment and existing knowledge as depicted in Figure 4.2.

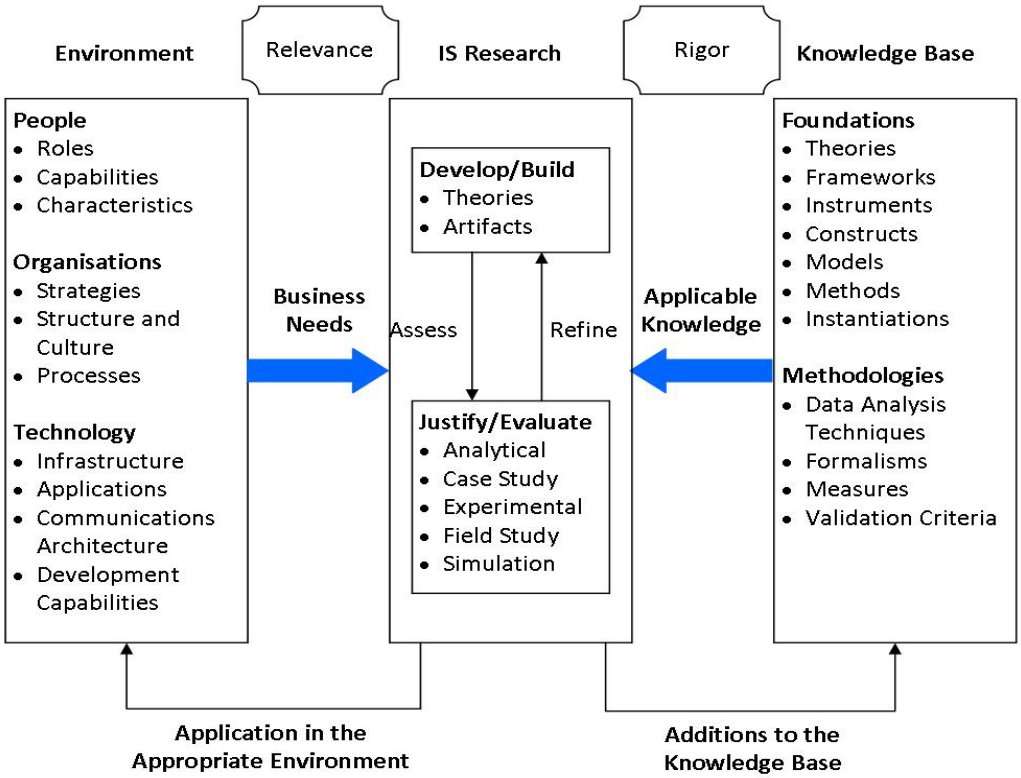


Figure 4.2: Information systems research framework (Hevner et al., 2004)

Hevner et al. (2004) acknowledge that IT artefacts design and evaluation have an impact on both the environment and on existing knowledge. The environment encompasses people, organisational processes and technology. In this study, the people include management, employees and the organisation's stakeholders. The organisation's processes of developing information security policies are also crucial. The knowledge base includes theories, framework, constructs and models, while methodologies encompass data analysis technique, formalism, measures and validation criteria.

4.1.6 Selection of a research paradigm appropriate for this research project

Based on the previous discussion of the different paradigms, this study aligns itself with the pragmatism paradigm while acknowledging the important influence of the Design Science paradigm. The pragmatism research paradigm is chosen because it supports the mixed method approach. Cameron (2011, p. 4) defines 'mixed methods' as "philosophical assumptions that guide the direction of the collection and analysis of data and the mixture of qualitative and quantitative data in a single study or series of studies."

Firstly, this study adopted a qualitative approach during the content analysis of existing theories and methods of developing information security policies. The objective of the

content analysis was to gather from the relevant literature the opinions and ideas about the methods available as regards developing an organisation's information security policy. The interpretation of the results of the content analysis resulted in the development of a conceptual framework for the information security policy development life cycle. Secondly, this research study uses a quantitative approach to validate the reliability of the proposed framework.

In addition, the Design Science paradigm was chosen for the purposes of the study because it provides comprehensive guidelines as regards designing IT artefacts. The main objective of this study was to develop a maturity assessment framework for the information security policy development life cycle and, thus, it was felt that the Design Science paradigm, which offers guidelines steps on designing and evaluating IT artefacts, could play a significant role in realising the objective of the study. March and Gerald (1995) differentiate between Design Science and natural science by stating that "design scientists strive to create models, frameworks, methods, and implementations that are innovative and valuable; while natural science is concerned with explaining how and why things are."

4.2 Research design

This research project followed the design science guidelines for producing and evaluating the end output solution. According to Peffers et al. (2008), Design Science Research involves a rigorous process, designing artefacts in order to solve observed problems, make research contributions, evaluate the designs, and communicate the results to appropriate audiences. The literature mentions various approaches that researchers and practitioners may adopt when designing and evaluating IT artefacts. The study conducted by Ahmad et al. (2011) contains rich information on the steps of Design Science implementation. However, this study follows the most widely cited guidelines of Design Science proposed by Hevner et al. (2004). Hevner et al. (2004) suggest seven guidelines that describe the characteristics of a well-executed design science research project. These guidelines are summarised in Table 4.4.

Table 4.4: Design Science guidelines (Hevner et al., 2004)

Design Science Guideline	Guideline objective
Guideline 1: Design as an artefact	Design science research must produce a viable artefact in the form of a construct, model, method, or an instantiation.
Guideline 2: Problem relevance	The objective of design science research is to develop technology-based solutions to important and relevant business problems.
Guideline 3: Design evaluation	The utility, quality, and efficacy of a design artefact must be rigorously demonstrated via well-executed evaluation methods.
Guideline 4: Research contributions	Effective design science research must provide clear and verifiable contributions in the areas of the design artefact, design foundations, and/or design methodologies.
Guideline 5: Research rigor	Design science research relies upon the application of rigorous methods in both the construction and evaluation of the design artefact.
Guideline 6: Design as a search process	The search for an effective artefact requires utilising available means to reach desired ends while satisfying laws in the problem environment.
Guideline 7: Communication of research	Design science research must be presented effectively both to technology-oriented as well as management-oriented audiences.

Hevner et al. (2004) advise that researchers, reviewers and editors must use their creative skills and judgement to determine when, where and how to apply each of the guidelines in a specific research project.

4.2.1 Application of the Design Science guidelines to this research project

The seven Design Science guidelines proposed by Hevner et al. (2004) are now discussed in terms of the way in which they were applied to solve the problem posed in this research project.

4.2.2 Problem relevance (Guideline 2)

The main objective of the problem relevance guideline is to define the specific research problem and to justify the value of the solution. Hevner et al. (2004) argue that research must address the problems and the opportunities arising from the interaction between people, organisations, and information technology. The research problem to be addressed in this study was the fact that there is no comprehensive mechanism for evaluating the processes involved in developing and implementing information security policies. The study made use of an extensive literature review and existing theories in order to identify the problem relevance.

4.2.3 Research rigour (Guideline 5)

Design Science research requires the application of rigorous methods in both the construction and the evaluation of the designed artefact (Hevner et al., 2004). This study used literature reviews, a content analysis of the secondary data, a survey and expert review to ensure a rigorous research methodology. A rigorous methodology was also used during the data collection and data analysis processes.

4.2.4 Design a search process (Guideline 6)

Hevner et al. (2004) maintain that Design Science is a search process aimed at discovering an effective solution to a problem. This may, in turn, be achieved by using an iterative approach that will lead to the most optimal solution. In this study the proposed framework was redefined based on the feedback from the security professionals that was collected from the open ended questions in the survey. In addition, an expert review was conducted in order to gain the views of the experts on improving the framework. Their feedback was incorporated into the framework.

This guideline was met through the use of a content analysis research technique in order to critically investigate the existing literature on information security policy development and implementation methods. In addition, the model which had been developed was then refined based on the input from the security professionals who had responded to the survey questionnaire instrument.

4.2.5 Design artefact (Guideline 1)

According to Denning (1997, p. 7), “Artefacts are innovations that define the ideas, practices, technical capabilities, and products through which the analysis, design, implementation, and use of information systems can be effectively and efficiently accomplished.” The interpretation of the results of the content analysis produced a conceptual framework. An in-depth literature study of the current security maturity models such as ISO/IEC 21827 and COBIT was conducted in order to highlight key processes that may be used in assessing the quality and maturity of information security policy development. The information derived from the content analysis was then collated in order to develop the framework solution for this study. The final output of the research project produced a process maturity assessment framework for the information security policy development life cycle.

4.2.6 Design evaluation (Guideline 3)

According to Peffers et al. (2008), the evaluation activities involve comparing the objectives of the solution with the actual observed results from the use of the artefact in the demonstration. In addition, Hevner et al. (2004) recommend that the utility, quality and efficacy of the artefact must be rigorously demonstrated via well-executed evaluation methods. The framework developed in this research project was evaluated by information security professionals in the field of information security management using a survey. In addition, an expert review was conducted in order to evaluate the framework.

4.2.7 Research contribution (Guideline 4)

The purpose of the final artefact was to integrate a security maturity assessment into the information security policy development life cycle. The framework ensured a comprehensive structured methodology for assessing the maturity levels of information security policy development life cycle. The contribution of this study is the research framework which will assist security policy developers to measure the effectiveness of their information security policy development life cycle.

4.2.8 Research communication (Guideline 7)

Finally, the results of the study will be published in journals and at conferences. Research communication enables practitioners to take advantage of the benefits offered by the artefact which has been produced (Hevner et al., 2004). In addition, the reviews of scientific papers may provide valuable input for further research contributions. Two papers from this study were presented at conferences – one at an international conference and the other at a local conference. Another paper has been submitted to a journal and is under the review process. This thesis will be available in the library of the University of Fort Hare. Figure 4.3 depicts the proposed sequence of the guidelines and the research process that was followed in order to achieve the objective of this study.

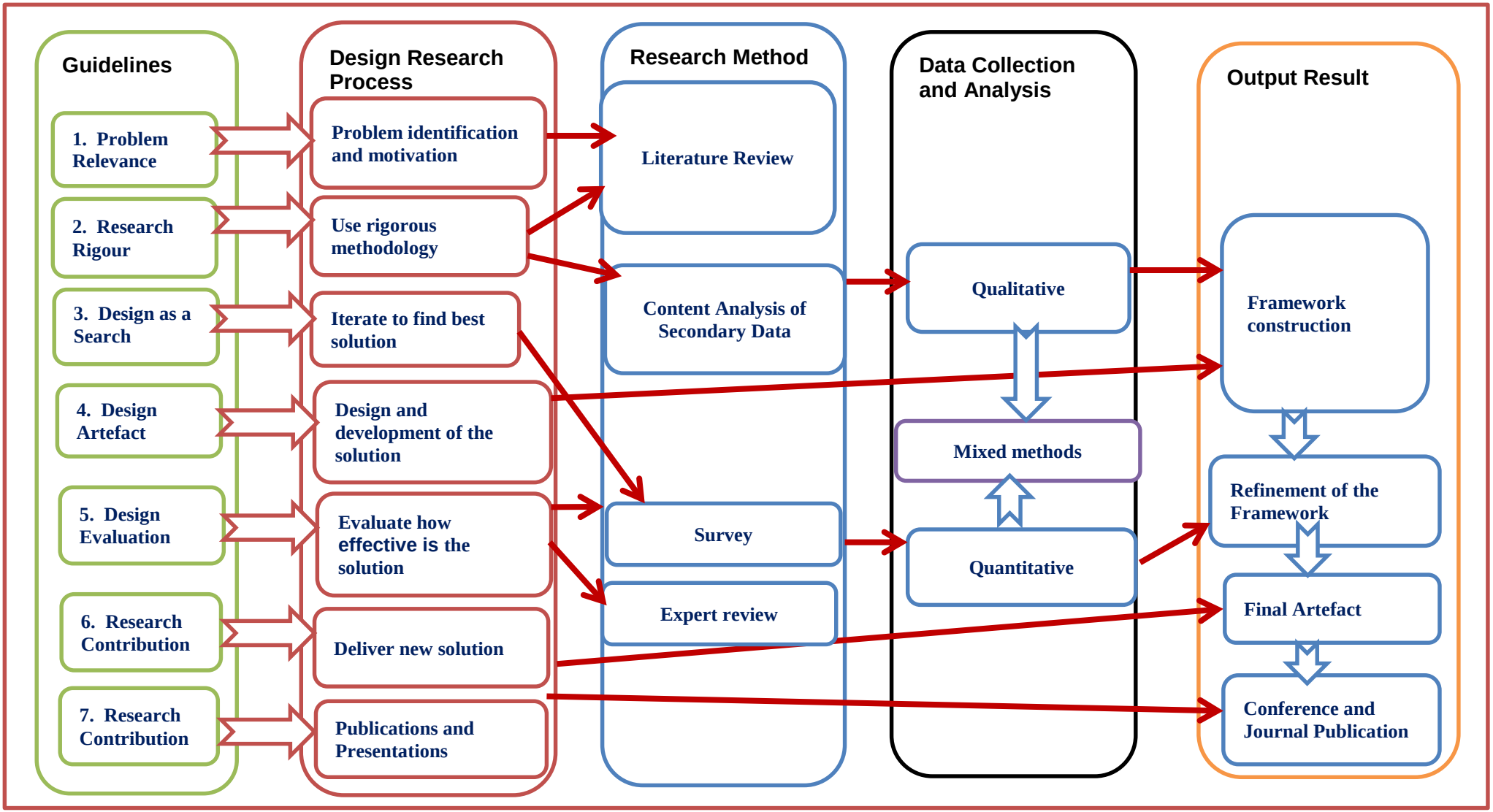


Figure 4.3: Application of Design Science to the study

4.3 Research approach

Saunders et al. (2009) maintain that the research process includes two possible approaches, namely, *induction* or *deduction*. According to Khalid et al. (2012, p. 4), "induction is the formation of a generalisation derived from the examination of a set of particulars, while deduction is the identification of an unknown particular, drawn from its resemblance to a set of known facts."

In terms of the inductive approach, the researcher moves from a particular observed situation to present broader, general ideas or theories. The researcher identifies patterns and regularities within the phenomena and progresses to formulate certain tentative hypotheses which are then explored and, finally, conclusions or theories are developed (Troachim, 2006). On the other hand, the deductive approach operates in the reverse direction to that of inductive reasoning. Mason (2002) highlights that, in deductive reasoning, theoretical propositions or hypotheses are generated in advance of the research process, and then changed through a process of either falsification or verification by the empirical research conducted.

In this study inductive logic was used to study relevant literature on existing information security policy development processes. The literature review, combined with the feedback information from security professionals, resulted in the formulation of the theory.

4.4 Research methods

There are three possible research methods which may be used to collect data, namely, *qualitative, quantitative* and *mixed method* (Morgan, 2007). This study may be said to have used a mixed method research methodology because it used both qualitative and quantitative methods during the data collection and data analysis processes.

According to Johnson and Onwuegbuzie (2004), mixed method research involves mixing or combining quantitative and qualitative research techniques, methods, approaches, concepts or language into one study. Oates (2006) explains that combining both research methods provides the researcher with multiple modes of "attack" on the research question. In addition, the findings or conclusions of such a study are more likely to be convincing and accurate than would otherwise have been the case (Yin, 2003).

In order to understand the mixed method approach, it is important firstly to discuss quantitative and qualitative approach. Blaikie (2000, p. 2) explains that "quantitative

methods are generally concerned with counting and measuring aspects of social life, while qualitative methods are more concerned with producing discursive descriptions and exploring social actors' meaning and interpretations." Oates (2008, p. 245) maintains that the objective of a quantitative data analysis is to look for patterns in the data and then to draw conclusions.

As illustrated in Table 4.5, Robson (2002) makes a comparison between the two research methods.

Table 4.5: Qualitative and Quantitative (Robson, 2002)

Quantitative	Qualitative
Used in research that requires facts and figures in order to answer the research question (through the verification of the hypothesis).	Deals mainly with the exploration of issues and the generation of theories within new and emerging subject areas.
Seeks to measure, test and quantify elements in order to explain or describe something.	Used to develop insight into and understanding of a subject.

In addition to the quantitative and qualitative approaches, the mixed method approach has emerged as an increasingly popular methodological choice for many academics and researchers from a variety of disciplines area (Cameron, 2011). According to Creswell and Clark (2007, p. 5), "mixed method's central premise is that the use of quantitative and qualitative approaches in combination provides a better understanding of research problems."

4.4.1 Mixed method

Creswell (2003, p. 245) suggests six different types of mixed methods design. These are referred to as strategies of inquiry that guide the choice of the type of mixed method to be used. The designs vary in terms of whether the qualitative and quantitative data is collected either sequentially or concurrently.

This study adopted the exploratory sequential design. The exploratory sequential design begins with and prioritises the collection and analysis of qualitative data. Building on the exploratory results, the researcher then conducts the quantitative phase of the study in order to test or generalise the initial findings. Firstly, the exploratory sequential design adopted for the purposes of this study explored the various processes of developing and implementing found in the literature using a content analysis technique. The results of the content analysis provided a conceptual framework for the information security policy development life cycle. Secondly, quantitative data collection was used to validate the

framework constructs with the objective of generalising the findings. Figure 4.4 depicts the exploratory sequential design used in this study.

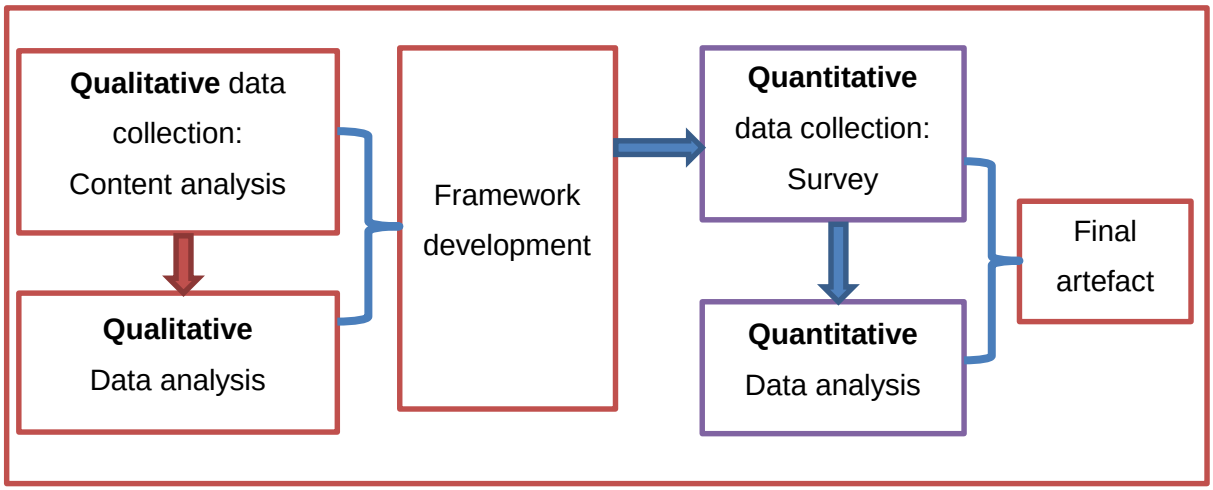


Figure 4.4: Exploratory sequential design

4.4.2 Secondary data collection: the content analysis research technique

The data which has been collected by a person other than the researcher in question is termed secondary data. A content analysis research technique was applied to the secondary data collected for the purposes of this study in order to find answers to the questions posed in the study. Krippendorff (2004, p. 10) defines content analysis as: "a research technique for making replicable and valid inferences from text to their context of use, with the purpose of providing knowledge, new insights, a representation of facts and a practical guide to action." However, Krippendorff (2004) goes further, explaining that the reference to text in this definition is not intended to restrict content analysis to written materials only as it may be used for arts, images, maps, signs and symbols as long as they communicate something about phenomena outside of what may be observed or sensed. There is a long history of content analysis being used in communication, journalism, sociology, psychology and business and, during the last few decades, there has been a steady increase in its use (Elo and Kyngas, 2007; Neundorf, 2002). The main objective of content analysis is to obtain a condensed and broad description of the phenomenon under investigation while the outcome of the content analysis is concepts or categories which describe the phenomenon (Elo and Kyngas, 2007).

It is essential that, as a research technique, content analysis follows a well-structured process in order to ensure reliability and validity (Du Preez and Botha, 2010).

Krippendorff (2004) mentions the following six steps that should be followed when conducting a content analysis, namely, *unitising, sampling, coding, reducing, inferring and narrating*. Figure 4.5 presents a graphical representation of the six steps of content analysis.

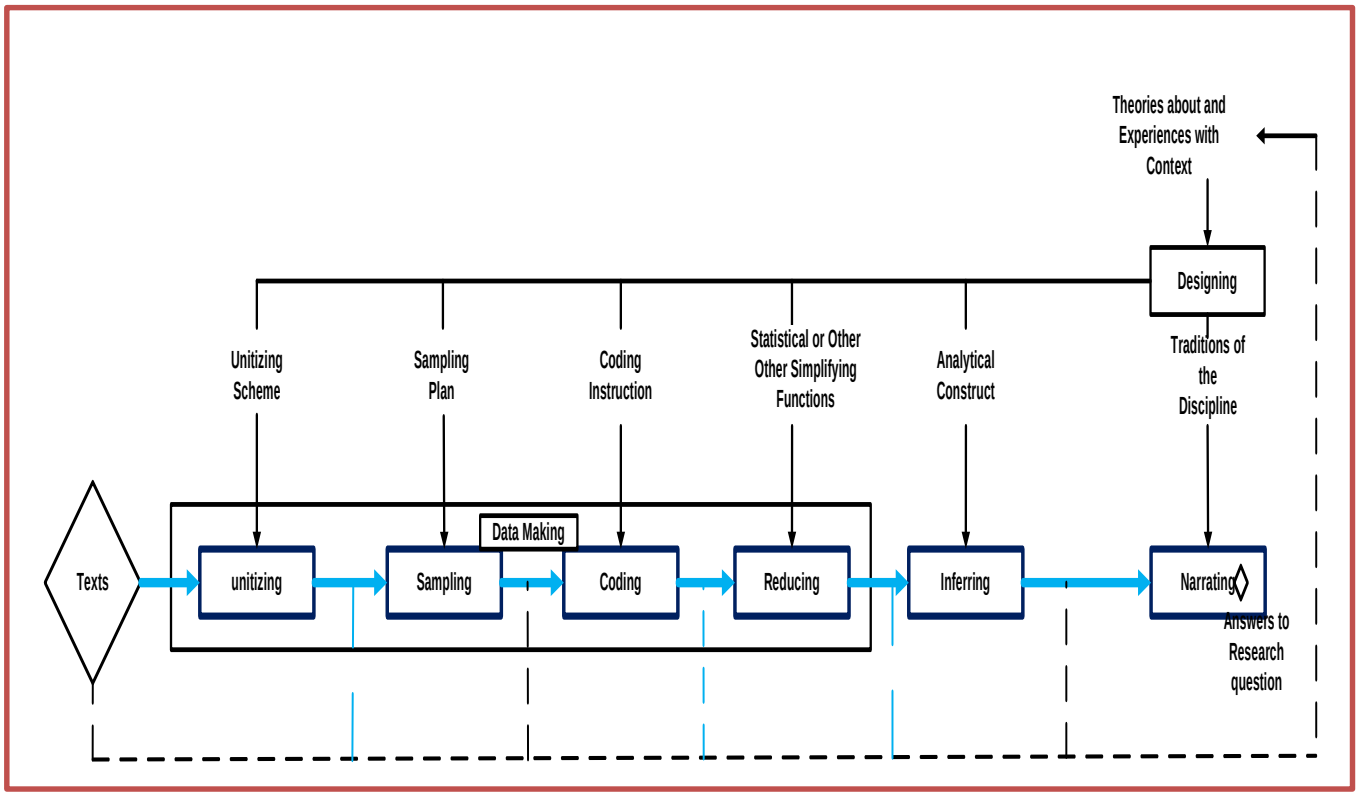


Figure 4.5: Six steps of the content analysis research technique (Krippendorff, 2004)

These six steps are described below with reference to the content analysis of information security policy development and implementation which was conducted in this study.

Step 1: Unitising

The process of content analysis begins with the creation of a scheme of categories which are composed of the various analysis units (Elo and Kyngas, 2007). A unit of analysis may be a word, sentence, or portion of words (Robson, 2002; Polit and Beck, 2004; Elo and Kyngas, 2007). Lopes and Sá-Soares (2010) argue that the more the units of analysis are clearly formulated and well adapted to the problem under study and content under analysis, the more productive the studies using content analysis will be (Berelson, 1952). Unitising refers to a systematic approach to distinguishing segments of texts that are of interest to a content analysis (Krippendorff, 2004). For the purposes of this study, search strings such as “security policy development”, “information security policy”,

"security policy implementation", "security policy formulation", "security policy creation", "security policy development process" were used to gather information regarding the security policy development and implementation methods from the literature.

Step 2: Sampling

Krippendorff (2004) highlights that sampling enables the content analyst to reduce his/her research efforts by cutting observations to manageable subsets of units that are, nevertheless, statistically or conceptually representative of the whole population. Ideally, the sample's findings should yield the same results as would the population from which the sample was drawn (White and Marsh, 2006). Accordingly, selecting the sample may be a daunting task. Du Preez and Botha (2010) advise that industry sources should not be overrepresented within the chosen sample merely because of their large representation within the population of texts.

Step 3: Coding

Coding entails the process of converting the texts from the sample into analysable units (Krippendorff, 2004). In order to avoid the possibility of human errors in this study, the coding step was conducted using the MAXQDA software package. MAXQDA is a software program which has been designed for computer-assisted qualitative and mixed methods data, text and multimedia analysis (MAXQDA, 2012).

Step 4: Reducing

Reducing is the fourth step in the content analysis process. The main objective of reducing is to decrease the number of codes into categories that may be easily interpreted (Krippendorff, 2004; Du Preez, 2010). The coding process often yields several codes and, thus, it becomes necessary to group these codes into various categories.

Step 5: Inferring

Inferring involves drawing conclusions about the particular phenomena under study. In this study, the reducing step produced a number of categories. An interpretation of those categories then resulted in the construction of a framework for the information security policy development life cycle.

Step 6: Narrating

Narrating is the last step in the content analysis process. The narrating process involves the way in which the inferences drawn from the content analysis provide answers to the research question(s) posed in the study. According to Krippendorff (2004, p. 11), "narration relies on the narrative traditions or discursive conventions established within the discipline of the content analyst." The next section discusses the primary data collection process which was conducted in the study.

4.4.3 Primary data collection based on the quantitative approach

The primary data collection in this study included a survey that was conducted in order to assess the importance of the information security policy development and implementation processes.

4.4.3.1 Survey

Leedy and Ormrod (2008, p. 183) define survey research as a method of collecting opinions, attitudes or previous experiences from a group of people by asking questions and tabulating their answers. The objective of a survey is to acquire information in order to be able to generalise about a population by surveying a sample of that population. Blumberg et al. (2008, p. 278) state that a survey is more efficient and economical as compared to observations if the aim of the researcher is to learn about the opinions and attitudes of the participants.

Gerber-Nel and Kotze (2003, p. 209) stress that it is essential that the sample size is large enough to ensure that reliability and validity conclusions may be drawn and which apply to the population from which the sample was drawn. For the purposes of this study a survey questionnaire was developed and distributed to 400 security professionals – 200 from the United Kingdom and 200 from the United States of America. A total number of 329 security professionals (192 from UK and 137 from USA) responded to the survey. The questionnaire was administered using the Surveymonkey software. The survey targeted information security professionals such as IT managers, chief information security officers and security specialists. The participants were chosen because they are involved in security related issues in their daily activities and, therefore, they may be considered to exert significant influence on the information security management of their organisations.

Design survey instrument

The design of the survey instrument was in accordance with advice and suggestions from the relevant literature. Olivier (2009, p. 81) suggests that a questionnaire should not ambiguous while researchers should make sure that the questions will be understood by the respondents (Funchall, 2011). In addition, the questions must be short and related items grouped together (Olivier, 2009, p. 82). Babbie (2005, p. 260) advises that the questionnaire should not be cluttered and that the same questions should not be repeated. It is important that the respondents do not become confused when completing the questionnaire. If the respondents do not understand a question they will either simply not answer it or give an incorrect answer so as to move on to another question.

The questionnaire used in this study was first piloted by a small group of six people in order to check for ambiguity, misleading, unclear terminology, or questions that were too long. The people who participated in the questionnaire pilot were colleagues who are researchers in information security field.

Research project survey focus area

The sources of the data in the questionnaire used in this research project were based primarily on the results of the content analysis that had been conducted on the secondary data which had been collected. Table 4.6 presents a summary of the way in which the questionnaire was constructed.

Table 4.6: Research project survey focus area

Objective	Measurement construct	Objective of measurement	Questionnaire reference
Demographic data	Name of country, Organisation type, Occupation, Organisation size	Demographic data	Q.1 – Q.5
Investigate the importance of the framework constructs	-Risk assessment -Security policy construction -Security policy implementation -Security policy monitoring -Security policy compliance -Employee support -Management support	Level of importance of the constructs	Q.6 – Q.12
Investigate the importance of the framework constructs sub-variables	- Assets identification - Vulnerability and threats - Risk identification - Legislation	Level of importance of risk assessment sub-variables	Q.13 – Q.16
	- Security policy audience - High level security policy - Detailed security policy - Lower level security policy	Level of importance of security policy construction sub-variables	Q.17 – Q.20
	- Security policy awareness - Security policy training - Stakeholders' role - Security policy education	Level of importance of security policy implementation sub-variables	Q.21 – Q.24
	- Periodic review - Automated review - Audit information - Non periodic review	Level of importance of security policy monitoring and assessment sub-variables	Q.25 – Q.28
	- Security policy approval - Security policy enforcement - Management involvement - Budget	Level of importance of management support sub-variables	Q.29 – Q.32
	- Deterrence measure - Binding agreement - Job termination - Employee involvement	Level of importance of employee support sub-variables	Q.33 – Q.36
	- Attitude - Perceived social pressure - Perceived benefit - Knowledge	Level of importance of security policy compliance sub-variables	Q.37 – Q.40

The next section discusses the survey's questions type.

Question types

The questionnaire contained open ended questions which gave the respondents the opportunity to give their own responses. The respondents were asked to offer suggestions in respect of the processes of developing and implementing information security policies that they felt were important but which had not been included in the questionnaire. For example: “Please add any activity that you feel is important with respect to the security policy implementation process within your organisation.”

In addition, the questionnaire also included closed ended questions consisting of Likert-type scale questions that restricted the respondents to selecting answers from a pre-defined question set. A Likert-type scale is based upon the assumption that each statement on the scale has the same attitudinal weight. The questionnaire used in this study may be found in Appendix B: Questionnaire.

4.4.3.2 Data analysis

While qualitative research considers the overall coherence and meaning of the data to be more important than the specific meaning of its parts, quantitative research uses statistical and mathematical techniques in order to observe specific variables in a data set (Mouton, 1996, p. 169). The data analysis used a triangulation process which combined the qualitative and quantitative data that had been used in the study. According to Guion (2002), triangulation is a method which is used by qualitative researchers to check and establish validity in their studies. Voce (2005) states that using a combination of data types (triangulation) increases the validity of a study as the strengths inherent in one approach may compensate for the weaknesses inherent in another approach.

Leedy and Ormrod (2001, p. 151) maintain that, during qualitative data analysis, the researcher starts by obtaining the raw data (structured or unstructured), organises and reduces the categories into groups and then compiles a final report. During content analysis process, this study followed the steps proposed by Leedy and Ormrod (2001, p. 151) and illustrated in Figure 4.6.

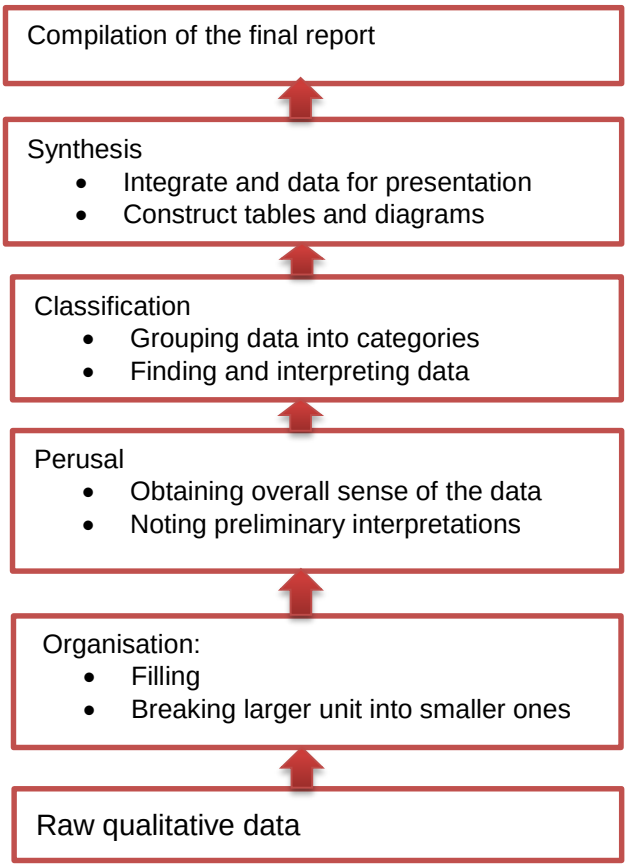


Figure 4.6: Data analysis spiral (Leedy and Ormrod, 2001)

The SPSS statistical package was used to conduct the statistical analysis in the quantitative phase of the study. Once the data had been entered in the SPSS, various statistical tests were conducted. Descriptive statistical tests were used to generate frequencies, the median, the mean and the standard deviation. In order to measure the reliability of the questions relating to the importance of the constructs of the proposed framework, Cronbach's Alpha was used. In addition, Pearson's correlation coefficient was used to investigate the relationship between the constructs of the proposed framework. The next section concludes this chapter.

4.5 Conclusion

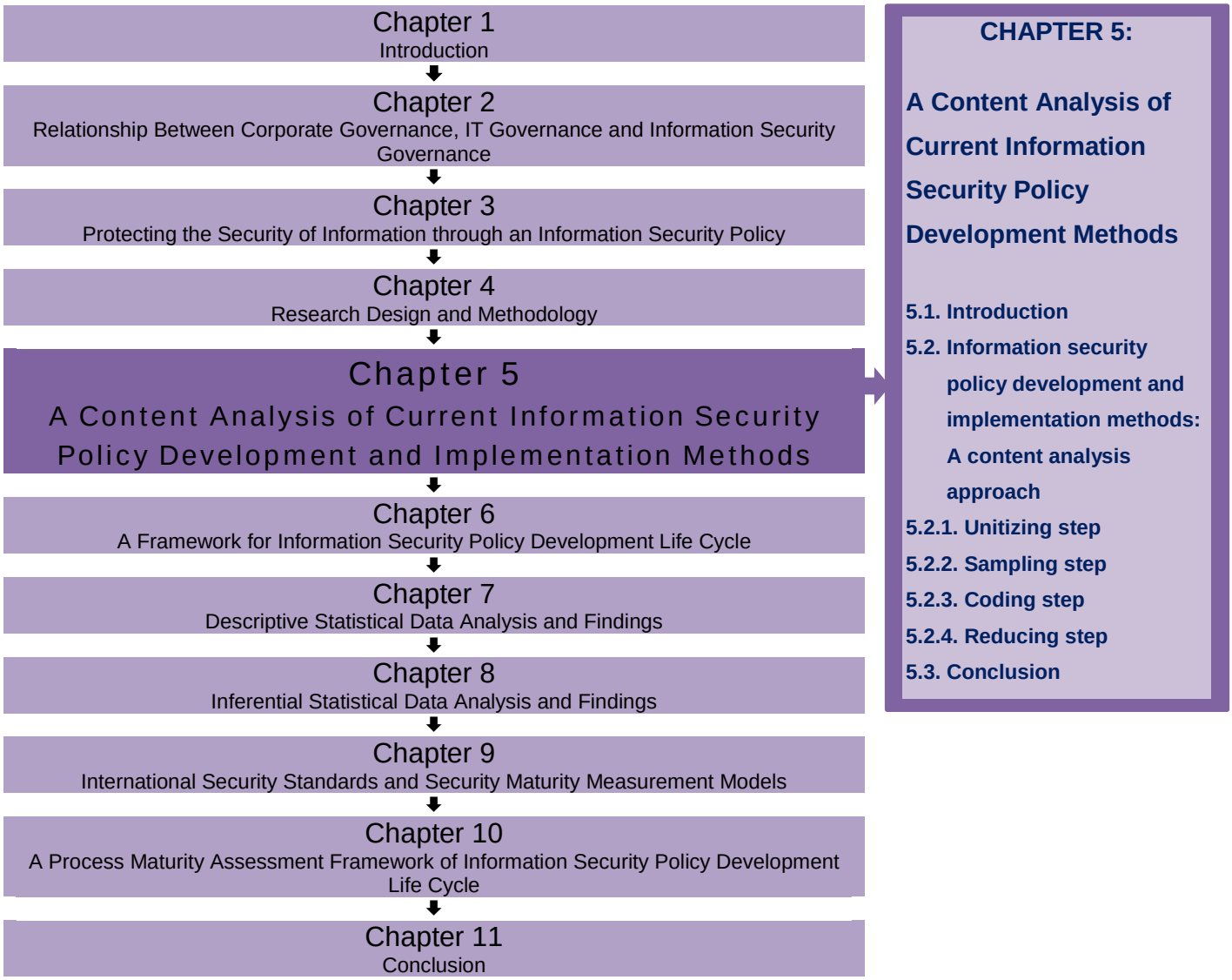
This chapter discussed the research methodology that was used for the purposes of this research project. The chapter discussed the various research paradigms. Based on the nature of the problem under investigation and the objectives of the study, this study was conducted within the pragmatism paradigm although there was also significant influence from the Design Science paradigm. The Design Science paradigm guided the research methodology and research design used. The research methodology comprised the mixed method approach. The study used the exploratory sequential design of the mixed

method approach and began with and prioritised the collection and analysis of the qualitative data. Building on the exploratory results of the qualitative data, the researcher then conducted the quantitative phase of the study in order to test or generalise the initial findings.

The chapter described the data collection methods used. A content analysis was conducted on the secondary data which had been collected in order to investigate the processes involved in developing and implementing information security policies. The primary data collection method was based on the quantitative data collection using a questionnaire. The chapter also discussed the data analysis process that was used.

Chapter 5 focuses on the secondary data collection method. In addition, the chapter discusses the content analysis of the information security policy development methods mentioned in the literature.

Chapter 5: A Content Analysis of Current Information Security Policy Development and Implementation Methods



5.1 Introduction

A review of relevant literature revealed a number of approaches that organisations may adopt in order to develop their own information security policies. Chapter 3 discussed the gap in the current security development methods and noted that the literature does not indicate the existence of a comprehensive methodology or mechanisms that demonstrate, in detail, the processes of constructing, implementing and implementing an information security policy. Accordingly, a more pragmatic strategy is clearly necessary. A content analysis of security policy development was conducted using the secondary sources in the literature in order to obtain a thorough understanding of the processes necessary for the formulation, implementation and application of an effective information security policy.

The research question posed in the study sought to ascertain the processes which organisations should follow in developing and implementing an effective information security policy. This study argues that an information security policy development life cycle, which comprises well-planned processes of security policy construction, implementation and enforcement, is vital to ensure the security of an organisation's information. This chapter describes the content analysis research technique that was used in order to answer the research question.

5.2 Information security policy development and implementation methods: A content analysis approach

According to Steve (2001, p. 26), content analysis is "a systematic, replicable technique for compressing many words of text into fewer content categories based on explicit rules of coding." This chapter analyses the various words and sentences related to information security development and implementation and places them into groups or categories. Figure 5.1 diagrammatically represents the way in which available texts may be subjected to the content analysis mechanism in order to answer a research question. The chapter also discusses the six steps of the content analysis research technique which were followed in order to answer the research questions posed in this study.

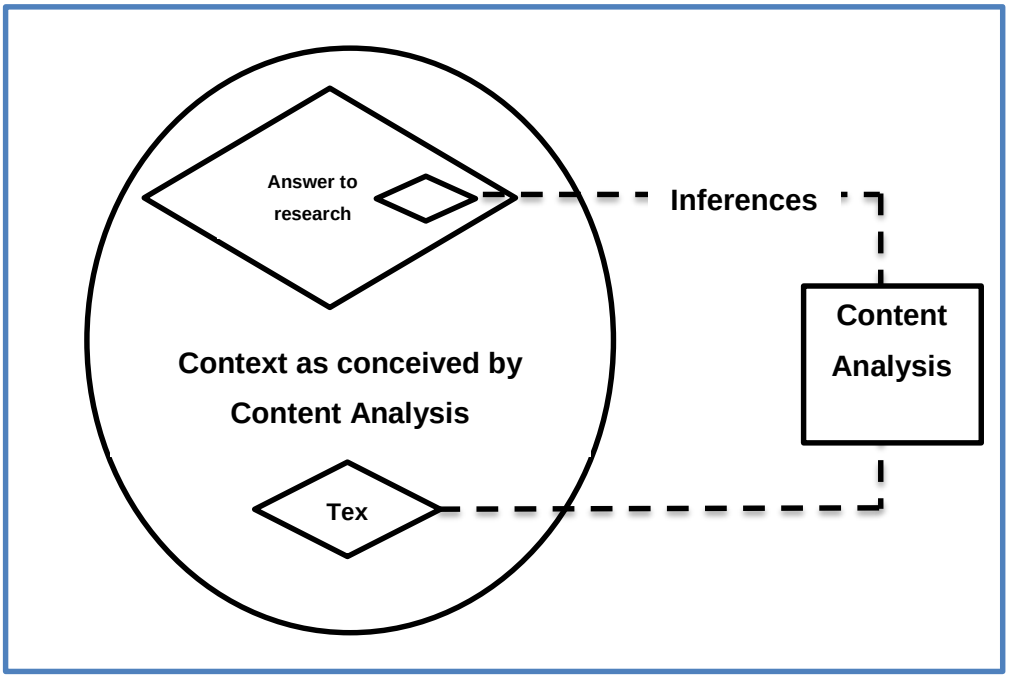


Figure 5.1: The content analysis research technique (Krippendorff, 2004)

Krippendorff (2004) highlights the six steps that should be followed while conducting a content analysis, namely, **unitizing, sampling, coding, reducing, inferring** and **narrating.**

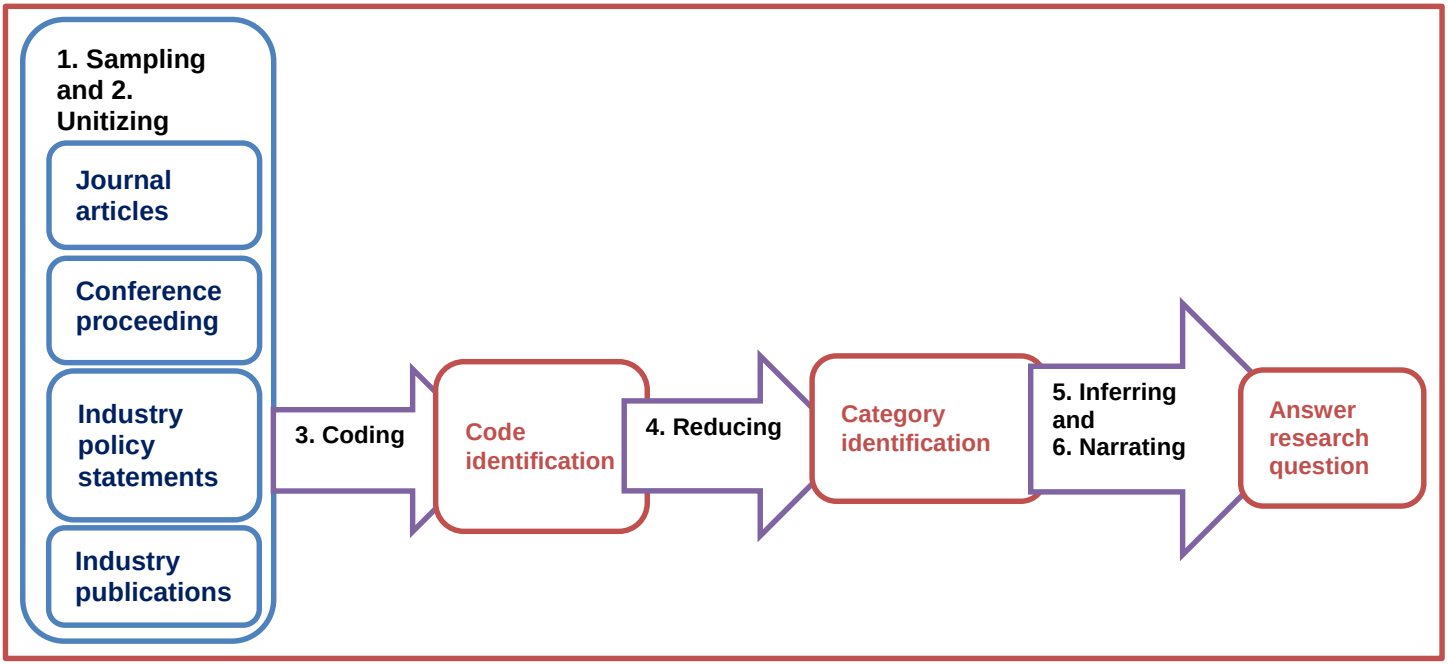


Figure 5.2: Content analysis steps (Krippendorff, 2004)

A discussion of the way in which the six steps of the content analysis were applied in this research project follows.

5.2.1 Unitising step

A content analysis on information security policy was conducted on the secondary sources in the literature. A total of 433 000 results were retrieved from a search which was conducted with the string "information security policy" on the search engine Google while 4 800 results were retrieved from Google Scholar. The search update for these given results took place on 6 August 2013. However, the number of results will definitely increase as more publications become available on the internet. Based on the high number of results, it was essential to select a manageable sample in order to conduct the content analysis.

5.2.2 Sampling step

According to Krippendorff (2004), sampling refers to drawing a manageable set of texts from the population when it is unrealistic to perform a content analysis on the entire population of texts. Having realised the important role of information security policies in protecting an organisation's information, there is an increasing number of business industries which are specialising in developing security policy content templates. For example, InformationShield Inc has an information security policy sample library containing 1 400 sample policies (InformationShield, 2013) and this, in turn, increases the number of sources on the internet. Accordingly, a strategic plan was required which would ensure a combination of the sources required when selecting the sample from the population of texts. Thus, this study used academic journals articles, conference proceedings papers, industry publications and industry policy statements in an effort to answer the research question.

During the selection of the sample, the reputation of the authors of the articles, and which depended, for example, on the number of people who had cited the articles, was taken into account. The reputation of the journal or the conference was considered. However, most importantly, those publications that contained relevant content directly related to the research topic under study were selected. This entailed an extensive analysis of the literature review. For the purposes of the study, a total number of 21 documents were chosen to make up the sample. These documents included the most frequently cited papers on Google. Table 5.1 presents a summary of the source of each paper and the justification for selecting that particular paper.

Table 5.1: Sample of information security policy development and implementation methods

1	**Source**	Talbot, S., Woodward, A. (2009). Improving an organisation's existing information technology policy to increase security. Proceedings of the 7th Australian Information Security Management Conference, 7(9), 120–128.
	Category	Conference proceeding paper
	Justification	This research paper examined the implementation of security policies in an organisation. The paper makes recommendations on the processes involved in improving an organisation's culture; creating an awareness mechanism for policies; reviewing the policy periodically; updating the policy; policy compliance and policy enforcement. All these recommendations are critical for security policy implementation.
2	**Source**	InstantSecurityPolicy.com (2013). The IT Security Guide: Why need one, what it covers, and how to implement it. Retrieved 11 June, 2014 from http://www.instantsecuritypolicy.com/Introduction_To_Security_policies.pdf.
	Category	Industry publication
	Justification	This paper was chosen because it discusses the integration of security policy creation processes with a business management model in terms of which the security risks may be easily quantified.
3	**Source**	Abdel-Aziz, A. (2010). How to review and assess information security policy: The Six-Step Process. Retrieved 15 May, 2013 from: http://www.sans.edu/.
	Category	Industry publication
	Justification	This paper was chosen because it addresses the information security policy review and assessment.

4	**Source**	Hong, K. S., Chi, Y. P., Chao, L. R., and Tang, J.H. (2006). An empirical study of information security policy on information security elevation in Taiwan. Information Management and Computer Security, 14(2), 104–115.
	Category	Journal article publication
	Justification	The finding of this paper highlights that organisations should focus on procedures and implementation items, rather than on the policy documents only. The contribution of this paper is relevant to the objectives of this study.
5	**Source**	Von Solms, R., Thomson, K. L., and Maninjwa, P.M. (2011). Information security policy governance through comprehensive policy architectures. In Proceedings of the Information Security for South Africa Conference. Johannesburg, South Africa.
	Category	Conference proceedings
	Justification	Von Solms has published several articles in the field of Information Security Governance and may be considered as one of the leading academics in the field of information security. This paper stresses the importance of information security policy as the main control with which to mitigate information security threats. In addition, the paper highlights how the information security policy should be implemented based on the strategic, tactical and operational management levels.
6	**Source**	Kadam, A. W. (2007). Information security policy development and implementation. Information Systems Security, 16(5), 246–256.
	Category	Journal article publication
	Justification	This paper points out a wide range of issues which were considered important to the research objectives of this study, including the need to conduct a risk assessment, developing security policy and procedures' processes, and management support.

7	**Source**	Bayuk, J. (2009). How to write an information security policy. Retrieved from http://www.computerworld.com/article/2525539/security0/how-to-write-an-information-security-policy.html
	Category	Industry article
	Justification	Jennifer Bayuk has published numerous articles on information security management emphasising the importance of information security policy control. In addition, Bayuk has co-edited information security management books, for example: Enterprise information security and privacy; Stepping through the IS audit (2nd ed.) and Stepping through the InfoSec program.
8	**Source**	Avolio, F. M., Fallin, S., and Pinzon, D.S. (2007). Producing your network security policy. WatchGuard Technologies.
	Category	Industry publication paper
	Justification	This paper discusses the processes involved in writing a security policy to protect the network security. It emphasises that security policies should be initiated by top managers. Furthermore, it highlights that, before writing a security policy, it is essential that organisations take into account the regulations that apply to that specific organisation. Accordingly, this paper was chosen to be part of the sample.
9	**Source**	Chen, H., and Li, W. (2014). Understanding organisation employees' information security omission behaviour: An integrated model of social norm and deterrence. Proceedings of PACIS 2014, Chengdu, China.
	Category	Conference proceedings
	Justification	The paper emphasises that deterrence measures will effectively decrease omission behavioural intention.

10	Source	Wahsheh, L. A., and Alves-Foss, J. (2008). Security policy development: Towards a life-cycle and logic-based verification model. American Journal of Applied Sciences, 5(9), 1117–1126.
	Category	Journal article paper
	Justification	The paper presents a model which describes the engineering processes of developing security policies.
11	Source	Bulgurcu, B., Cavusoglu, H., and Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based belief and information security awareness. MIS Quarterly, 34(3), 523–548.
	Category	Journal article publication
	Justification	Based on the theory of planned behaviour, this article investigates the factors that drive an employee to comply with requirements of the information security policy. It also investigates the impact of information security awareness on an employee's outcome beliefs. Information on both information security policy compliance and security awareness contributed significantly to answering the research question posed in this study.
12	Source	RSA Security Inc. (2009). A guide to security policy: A primer for developing an effective policy. Retrieved 10 May, 2013 from: www.sans.org/security-resources/policies/Policy_Primer.pdf.
	Category	Industry policy publication
	Justification	This paper discusses important factors related to security policy implementation such as policy communication and policy enforcement. Accordingly, this paper was chosen for the sample because of its critical contribution to the main objective of the research project.

13	Source	Karyda, M., Kiountouzis, E., and Kokolakis, S. (2005). Information systems security policies: A contextual perspective. Computers and Security, 24(3), 246–260.
	Category	Journal article publication
	Justification	This paper explores the processes involved in formulating, implementing and adopting a security policy in an organisation. The paper looks specifically at the contextual factors that affect the successful adoption of information security policies.
14	Source	National Computer Board. (2011). Guideline on information security policy. Retrieved 12 June, 2014 from http://www.ncb.mu/English/Documents/Downloads/Reports%20and%20Guidelines/Guideline%20on%20Information%20Security%20Policy.pdf.
	Category	Government policy report
	Justification	This report is important because it points out that there are different policy audiences in every organisation and, therefore, that it is imperative that the development of security policy take this issue into account. The report also mentions the responsibilities of the various stakeholders in security policy development.
15	Source	University of Newcastle (2009). Policy development and review process: Guideline. Retrieved 12 January, 2013 from: http://www.newcastle.edu.au/Resources/Divisions/Services/Corporate%20Governance/Policy/Policy-Development-Guideline.pdf.
	Category	Academic policy statements
	Justification	The document cites the processes which are required during the policy review, drafting the policy and policy consultation. It also highlights the roles of stakeholders in approving the security policy.

16	**Source**	Diver, S. (2007). Information security policy: A development guide for large and small companies. Retrieved 15 June, 2013 from: http://www.sans.org/reading-room/whitepapers/policyissues/information-security-policy-development-guide-large-small-companies-1331.
	Category	Industry policy publication
	Justification	This paper offers a unique perspective that the other papers in the sample did not offer. It emphasises the need to consider regulatory requirements before developing security policies. The paper also recommends taking into account the current security policy maturity before choosing which approach to follow in developing security policy.
17	**Source**	Al-Awadi, M., and Renaud, K. (2007). Success factors in information security implementation in organisations. Proceedings of IADIS International Conference e-Society, 169–176.
	Category	Conference proceeding paper
	Justification	The paper highlights the important factors to be considered during the implementation of an information security policy. These factors include awareness and training, management support, budget and information security policy enforcement and adaptation. All these factors were crucial in this research project.
18	**Source**	Griffins, M. (2009). How to write a policy manual. Retrieved 12 July, 2013 from: http://www.templatezone.com/download-free-ebook/office-policy-manual-reference-guide.pdf
	Category	Industry policy publication
	Justification	The paper discusses the various steps involved in writing policies and in the approval process. It also discusses the processes involved in distributing new security policies.

19	**Source**	Corpuz, M.S., and Barnes, P. (2010). Integrating information security policy management with corporate risk management for strategic alignment. In Proceedings of the 14th World Multi-Conference on Systemics, Cybernetics and Informatics (WMSCI 2010), Orlando, Florida.
	Category	Conference proceedings paper
	Justification	The objective of this paper was to integrate information security policy management with corporate risk management. The paper also mentions the various risk assessment processes which were critical to this research project.
20	**Source**	Yayla, A. (2011). Controlling insider threats with information security policies. In Proceedings of 19th European Conference on Information Systems: ECIS, Helsinki, Finland, pp. 242–257.
	Category	Conference proceedings paper
	Justification	This paper discusses different socio-behavioural control mechanisms that are useful in mitigating insider threats to information security. These include, for example, deterrence measures that may be used to ensure that employees do not violate the organisation's rules.
21	**Source**	Khan, R. (2010). Practical approaches to organisational information security management. Retrieved 15 June, 2014 from http://www.sans.org/reading-room/whitepapers/leadership/practical-approaches-organisational-information-security-management-33568.
	Category	Industry policy publication
	Justification	This paper emphasises the importance of the information security policy communication and publication within an organisation. It also points out the need for detailed process documentation of information security programme.

After the sample has been established, the coding process commences.

5.2.3 Coding step

The coding was carried out using MAXQDA. MAXQDA is a qualitative data analysis software package which is used to code and interpret the data (MAXQDA, 2012). The twenty one sample documents were imported into the MAXQDA software. Each document was individually coded. The coding process involved first manually highlighting the sentence or paragraph that contained mention of the process of developing security policy. This process of highlighting texts and applying codes to such texts is known as tagging.

As depicted in Table 5.2, the findings of the coding steps revealed 29 codes and 628 cumulative tags. In addition, there was a variation of the codes from the general to the specific. For example, the general code was risk assessment while the specific codes included: identify the threats, identify the vulnerabilities and identification of the assets to be protected. The codes were grouped under one category in the next stage – the reducing step. Table 5.2 presents the results of the codes that emerged during the coding process.

Table 5.2: Emerged codes

Code no	Code label	No of tags	Cumulative tags
1	Write high level security policy	40	40
2	Write detailed security policy	28	68
3	Write lower level security policy	28	96
4	Information security policy consultation	17	113
5	Information security policy training	28	141
6	Information security policy awareness	29	170
7	Information security policy education	20	190
8	Stakeholders' roles	8	198
9	Perceived benefit of compliance	21	219
10	Knowledge	25	244
11	Attitude	20	264
13	Perceived social pressure	23	287
14	Identification of assets to be protected	24	311
15	Identification of risk	20	331
16	Identification of threats and vulnerability	19	350
17	Legislative requirements	21	371
18	Periodic review of security policy	16	387
19	Non periodic review of security policy	20	407
20	Automated review	18	425
21	Review of the audit information	13	438
22	Employee involvement	45	483
23	Sign binding agreement	12	495
24	Job termination	13	508
25	Deterrence measures	22	530
26	Management involvement	36	566
27	Budget	15	581
28	Information security policy approval	27	608
29	Information security policy enforcement	20	628

Once the coding process has been accomplished, the next stage is the reducing step.

5.2.4 Reducing step

The main objective of reducing is to decrease the number of codes into categories that may then be easily interpreted (Du Preez and Botha, 2010). The 29 categories that had emerged during the coding process were reduced to seven categories with some of the smaller categories being merged with similar allied categories. For example, the codes labelled "identification of vulnerabilities", "identification of threats", "identification of assets

to be protected" and "legislations" were grouped under one category termed 'risk assessment' as they were all part of evaluating the security risk processes. Table 5.3 depicts the categories which were identified.

Table 5.3: Categories identified

Category label	Number of tags	Cumulative tags
Information security policy construction	113	113
Management support	98	211
Employee support	92	303
Information security policy compliance	89	392
Information security policy implementation	85	477
Risk assessment	84	561
Information security policy monitoring and assessment	67	628

The categories presented in Table 5.3 may be considered as the main pillars of the security policy development and implementation processes. The category with a high frequency of occurrence was related to the process of information security policy construction. There was also a high frequency of both management support and employee support as most of the sources mentioned the involvement of these two factors in the information security policy development and implementation process. Figure 5.3 provides a graphical representation of the categories identified.

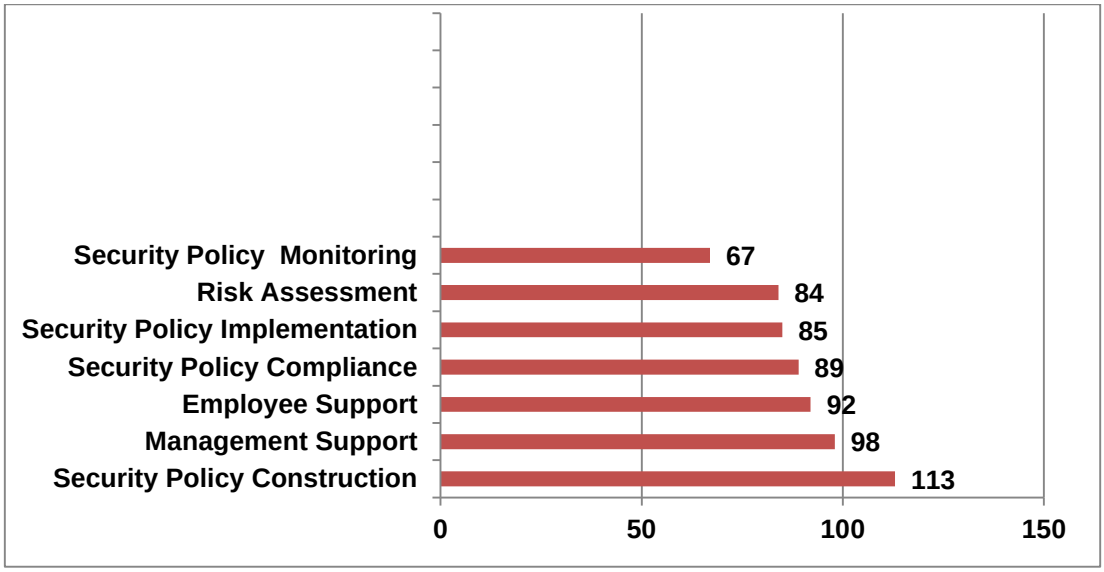


Figure 5.3: Identification of categories

These seven categories that were identified will be briefly discussed individually in the following section.

5.2.4.1 Information security policy construction category

One of the categories that emerged during the coding process with the highest number of tags was the writing of the security policy with a total number of 113 tags. In view of the fact that the chosen sample addressed information security policy development, it is not surprising that there were such a high number of tags in this category. This category comprises the codes related to the steps required in constructing an information security policy. These codes included write high level security policy; write detailed security policy; write lower level security policy; and consultation with information security policy stakeholders.

Table 5.4: Information security policy construction category

Category	Code name
Information security policy construction	Write high level security policy
	Write detailed security policy
	Write lower level security policy
	Consultation with stakeholders

Information security policy construction is the stage in which the security policy developers go through the processes of drafting a security policy, writing a security policy and obtaining management approval of the new security policy. The information policy construction process is triggered by both the findings and the recommendations of the risk assessment plan and are the next step after the risk assessment process has been accomplished. Anand (2012) emphasises that it is vital that organisations formulate information security policies in order to encounter the threats that have been identified during the risk assessment process.

5.2.4.2 Management support category

One of the categories that emerged during the coding process was the management support category. Management support had second highest number of tags and included a total number of 98 tags. The following code names made up the management support category, namely, management involvement; budget; information security policy approval; and information security policy enforcement.

Table 5.5: Management support category

Category	Code name
Management support	Information security policy approval
	Information security policy enforcement
	Management involvement
	Budget

The next section discusses the risk assessment category.

5.2.4.3 Risk assessment category

The codes that made up the risk assessment category included the following: identification of the threats; assessment of the threats; identification of vulnerabilities; assessment of vulnerabilities; assessment of impacts; identification of the assets to be protected; and risk identification.

Table 5.6: Risk assessment category

Category	Code name
Risk assessment	Assets identification
	Vulnerability and threats identification
	Risk identification
	Legislation

The next section discusses the information security policy implementation category.

5.2.4.4 Information security policy implementation category

This category encompassed all the code names related to information security policy implementation within an organisation. These codes included information security policy awareness; information security policy training; role of stakeholders; and information security policy education.

Table 5.7: Information security policy implementation category

Category	Code name
Information security policy implementation	Information security policy awareness
	Information security policy training
	Role of stakeholders
	Information security policy education

5.2.4.5 Information security policy monitoring and review category

The codes that made up the information security policy monitoring and review category included periodic review, automated review, review of the audit information; and non-periodic review.

Table 5.8: Information security policy monitoring and review category

Category	Code name
Information security policy monitoring and assessment	Periodic review
	Automated review
	Review of the audit information
	Non periodic review

In the selected sample, Griffins (2009), Talbot and Woodward (2009), Diver (2007) and Hong (2006) agree that the information security policy should be a "living document", which is dynamic and subject to change. Griffins (2009) describes the creation of an information security policy as a form of research which is an on-going aspect of keeping the information security policies up-to-date.

5.2.4.6 Employee support category

The code names that made up the employee support category included deterrence measure; binding agreement; job termination, and employee involvement. In the chosen sample, Chen and Li (2014) propose a theoretical model which integrates general deterrence and social norm theory. Their proposed model argues that deterrence measures will effectively decrease omission behavioural intention.

Table 5.9: Employee support category

Category	Code name
Employee support	Deterrence measure
	Binding agreement
	Job termination
	Employee involvement

The next section discusses the information security policy compliance category.

5.2.4.7 Information security policy compliance category

The code names that made up the information security policy compliance category included attitude; perceived social pressure; perceived benefit, and knowledge. In the chosen sample, Bulgurcu et al. (2010) discussed an information security policy compliance model which is based on the Theory of Planned Behaviour. The constructs of their proposed model included attitude; perceived social pressure; perceived benefit, and knowledge.

Table 5.10: Information security policy compliance category

Category	Code name
Information security policy compliance	Attitude
	Perceived social pressure
	Perceived benefit of compliance
	Knowledge

As mentioned in Chapter 3, this study relied on existing theories related to information security policy such as the Theory of Planned Behaviour. Accordingly, the model proposed model by Bulgurcu et al. (2010) may be regarded as relevant to this study as it looks at how the Theory of Planned Behaviour enhances compliance with information security policies.

5.3 Findings of the content analysis

The content analysis found that information security policy construction is the main step which should be conducted during an information security policy development life cycle. As depicted earlier in Figure 5.3, this step demonstrated the highest number of tags during the content analysis and was followed by management support and employee support. The roles of management and the employees are vital if an information security policy is to be successful in an organisation. The content analysis revealed that risk assessment and information security policy monitoring were the least important steps during an information security development and implementation process. This, in turn, reveals that there is a gap in the literature and, thus, the main objective of this study was to find a suitable solution to the problem of this gap. The next section discusses the validity and reliability of the content analysis which was conducted.

5.4 Validity and reliability of the content analysis

Miller (2008) defines reliability "as the extent to which a questionnaire, test, observation or any measurement procedure produces the same results on repeated trials". In this study the coding process was carried out by two researchers. At the end of the coding process, the results of the number of tags for each code label were compared to check whether there were discrepancies. If there were differences, a recount took place until the two researchers had reached agreement.

According to Miller (2008, p. 11), "validity refers to the extent to which an empirical measure adequately reflects what humans agree on as the real meaning of a concept." At the end of the coding process, the two researchers who had been involved in the coding of the documents verified that they had been coding for the same words. The results were compared and any discrepancies resolved. Thereafter, the final codes for the content analysis were produced as shown in Table 5.2.

According to GAO (1989, p. 14), "reliability and validity depend on the quality of information contained in the documents being analysed. If these are not reliable or valid, even the most rigorous content analysis will have limited value". Stemler (2001) suggests that the validity of a content analysis may be ensured by using multiple sources. In this study, academic journal articles, conference proceedings papers, industry publications and industry policy statements were chosen during the sampling step. The inclusion of these documents resulted in a representation of texts from multiple sources and this, in turn, enhanced the validity of the study. Furthermore, the use of MAXQDA during the coding process enhanced the reliability of the study as MAXQDA reduced the possibility of human error when calculating the frequency and occurrence of codes.

5.5 Conclusion

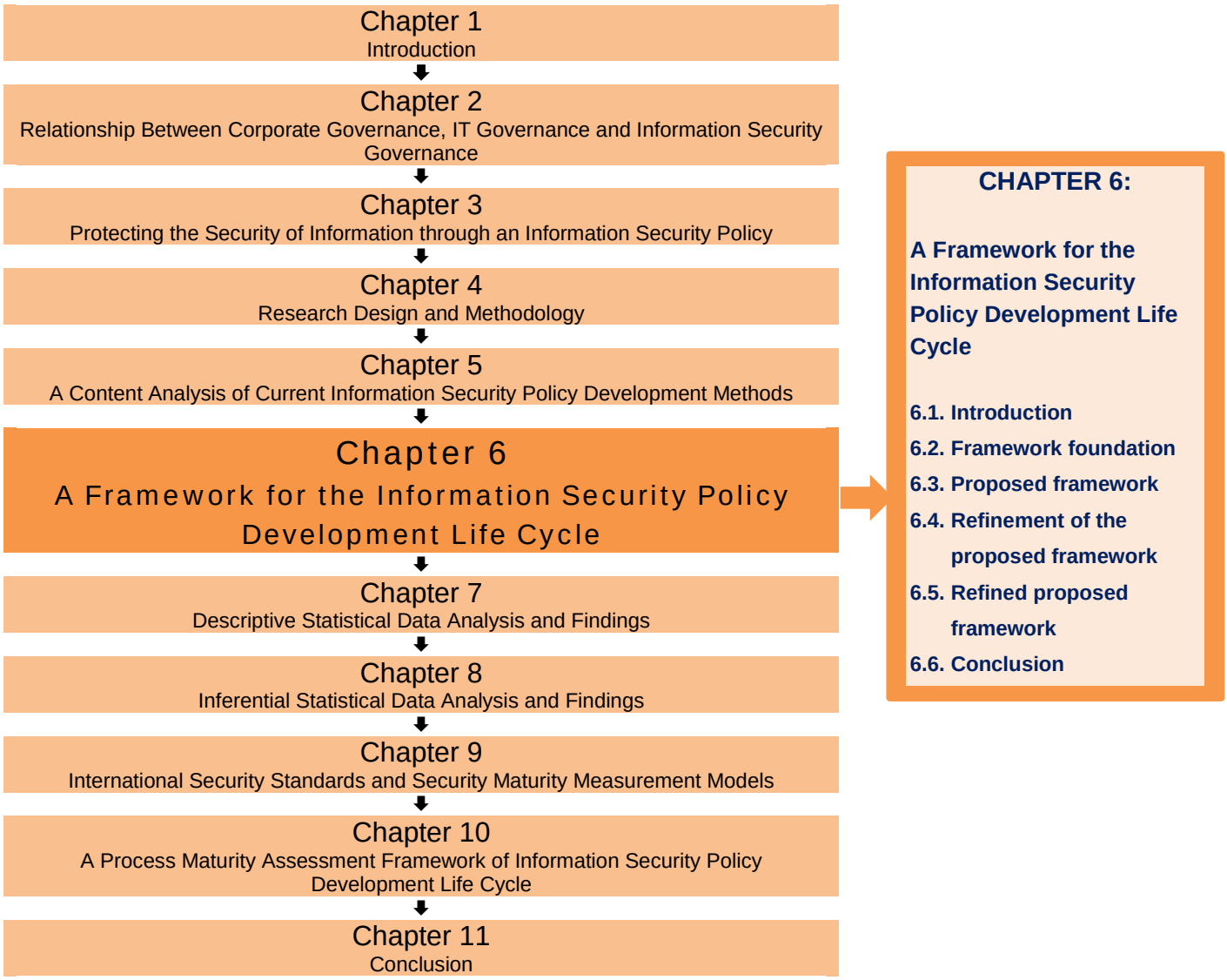
This chapter discussed how the four stages of the content analysis research technique were applied in this research project. These four stages include the unitising, sampling, coding and reducing stages. During the unitising and sampling 21 documents were chosen for the content analysis that was conducted. The sampling process ensured that the documents which were chosen represented texts related to information security development and implementation from the literature.

The discussion of the coding process disclosed how the researcher had coded the sample documents. The findings of the coding process revealed 29 codes and 628

cumulative tags. The reducing stages resulted in seven categories that constitute the main pillars of the information security policy development and implementation process. These are: information security policy construction, management support, employee support, information security policy compliance, information security policy implementation, risk assessment and information security policy monitoring and assessment.

The next Chapter, Chapter 6, focusses on the last two stages of the content analysis, namely, the narrating and inferring stages. The seven categories that emerged from the reducing stage are further discussed in Chapter 6 while a framework for the study is developed based on the interpretation of these categories.

Chapter 6: A Framework for the Information Security Policy Development Life Cycle



6.1 Introduction

The following research question was posed at the beginning of this study: What are the processes organisations should follow in developing an effective information policy? Unfortunately, the list of the seven categories that emerged during the reducing stage of the content analysis does not provide an answer to this question. Accordingly, it was necessary to analyse and interpret these seven categories so that an answer to the research question posed in the study could be inferred from the categories. The main objective of this chapter is to discuss these categories in depth.

This chapter discusses the final two stages of the content analysis, namely, **narrating** and **inferring**. Krippendorff (2004) points out that narrating the answers to content analysts' questions amounts to the researchers' making their results comprehensible to others. Thus, the narrating process deals with the way in which the inferences drawn from the content analysis provide answers to the research questions posed in a study. Within the context of this study the inferring step proposes a framework for the information security policy development life cycle and is based on the interpretation of the seven categories which emerged in Chapter 5.

6.2 Framework foundation

The BusinessDictionary (2004) defines a framework as "outline, or skeleton of interlinked items which supports a particular approach to a specific objective, and serves as a guide that can be modified as required by adding or deleting items." The framework proposed in this chapter is based on the integration of the existing information security policy development and implementation methods and models found in current literature. As discussed in Chapter 5, these models and methods were identified during the sampling step of the content analysis. This chapter proposes two stages of the framework. The initial framework is based on the results of the content analysis categories which were identified in Chapter 5. The second stage of the framework is the refined framework which incorporates the input of security professionals which was obtained from the survey conducted (see Chapter 7). Chapter 8 examined the relationship between the constructs. In addition, the refined framework includes the expert review comments (see Chapter 9). Figure 6.1 depicts the framework foundation chapters diagrammatically.

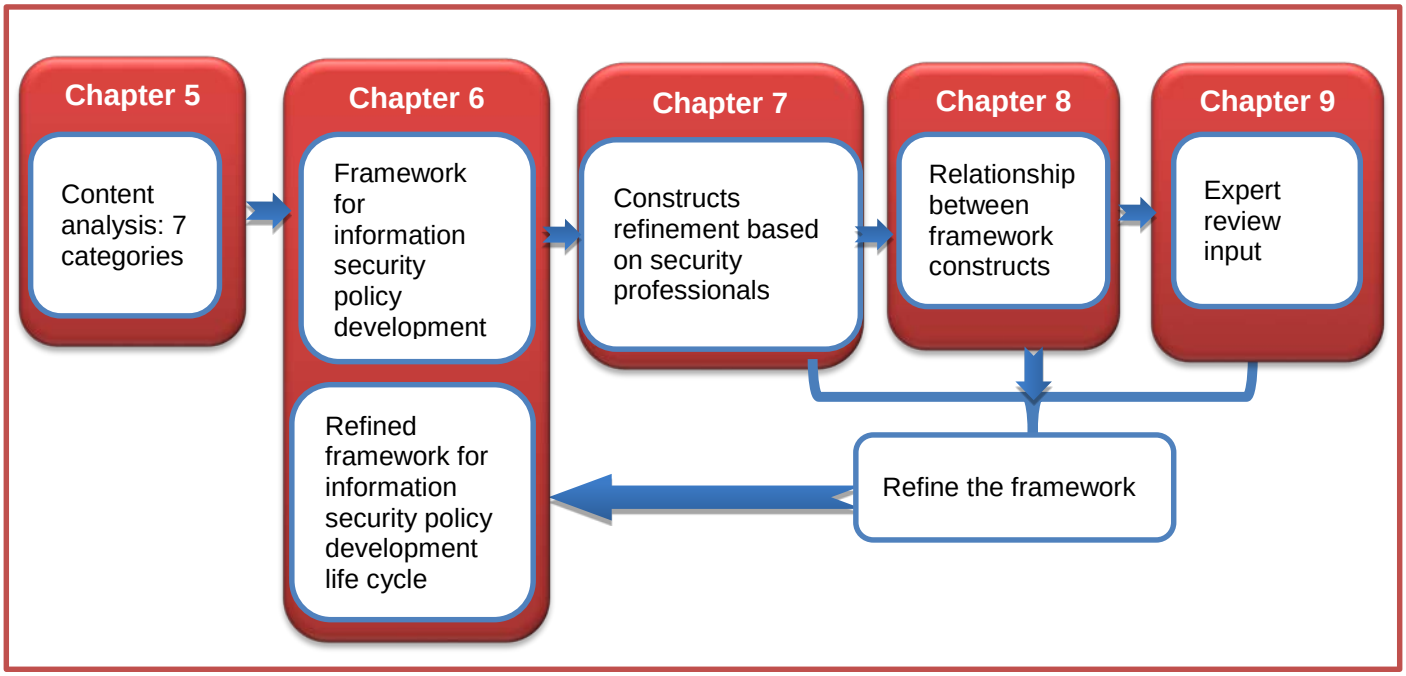


Figure 6.1: Framework foundation

The next section discusses the initial framework.

6.3 Initial framework

The proposed initial framework is based on the results of the content analysis categories. Table 6.1 depicts the seven constructs and the factors identified in relation to each construct.

Table 6.1: Initial framework constructs

Framework construct	Source	Factors identified
Risk assessment	Content analysis	Assets identification
		Vulnerability and threats assessment
		Risk identification
		Legislation
Information security policy construction	Content analysis	High level security policy
		Detailed security policy
		Lower level security policy
		Consultation with stakeholders
Information security policy implementation	Content analysis	Security policy awareness
		Security policy training
		Role of stakeholders
		Security policy education
Information security policy monitoring and assessment	Content analysis	Non periodic review
		Automated review
		Review of the audit information
		Periodic review
Information security policy compliance	Content analysis	Attitude
		Social pressure
		Benefit of compliance
		Knowledge
Management support	Content analysis	Policy approval
		Policy enforcement
		Management involvement
		Budget
Employee support	Content analysis	Deterrence measure
		Binding agreement
		Job termination
		Employee involvement

By looking carefully at the seven constructs, it was obvious that five constructs: Risk assessment, information security policy construction, information security policy implementation, information security policy compliance and information security policy monitoring and assessment encompasses all the processes needed to develop and implement an information security policy. Therefore, this dimension was called information security policy development life cycle dimension. The second dimension is the people dimension which is composed of management support and employee support. Based on the seven constructs and the twenty eight factors shown in Table 6.1, a framework is proposed in Figure 6.2.

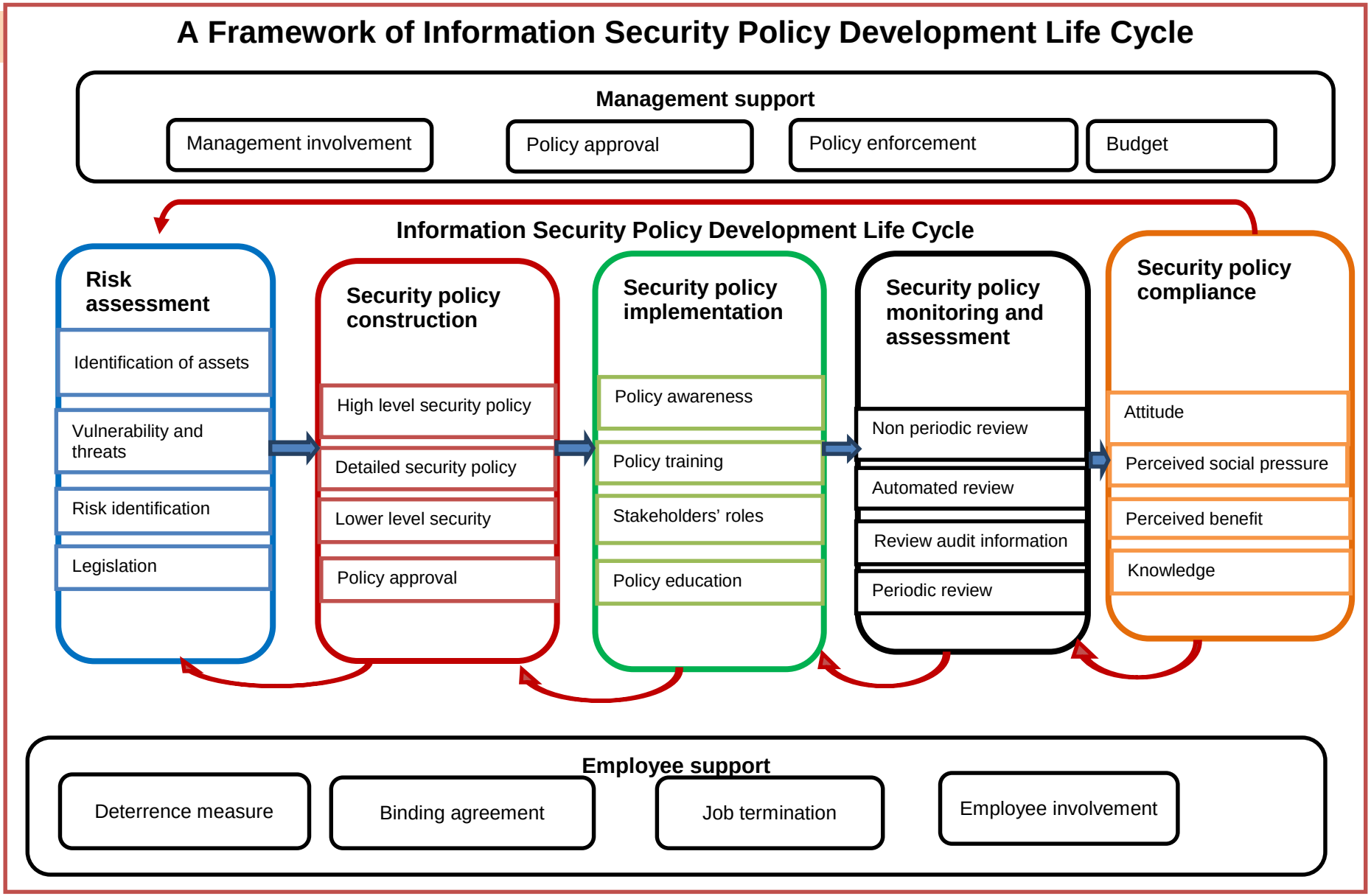


Figure 6.2: Initial framework

It is imperative that both management and employees support the information security policy if it is to survive and realise its objectives. The content analysis findings showed that management and employees support constructs had the highest frequency of tags after the information security policy construction construct.

In the proposed framework management support is depicted at the top of the diagram and, as an important component of a successful information security policy development life cycle, it spans all of the constructs. In the main, executive managers use policies to make known their management support and direction. "Without management supporting security policies, they might be as well be non-existent" (Jarmon, 2002, p. 11). However, it is essential that these policies are communicated to all staff members so that the staff members know what is expected of them.

The need for employee support is incorporated in the information security policy development life cycle diagram as a horizontal bar spanning the entire policy development life cycle. As stated in Chapter 2, employees are the weakest link in an organisation's information security and it is they who put the organisation at risk. Thus, employees need to know what they should and should not be doing, as individuals, in order to maintain the appropriate levels of security. Accordingly, there is an urgent need for a communication strategy between managers and staff members throughout the entire policy development life cycle.

Chapter 7 will explore the importance of management and employee support while Chapter 8 will focus on validating the assumption made in this chapter that there needs to be both management support and employee support throughout the entire process of the information security policy development life cycle. The next section discusses the refinement of the proposed framework.

6.4 Refinement of the proposed framework

The refinement of the framework was conducted in two stages. In the first stage, security professionals were asked to add new factors that they deemed to be important but which had been not included on the proposed framework depicted in Figure 6.2. Their inputs are discussed in Chapter 7 and are presented in Table 6.2. The second stage comprised an expert review process. A panel of seven expert reviewers was presented with the framework and asked to review the framework and suggest any construct or factors that they deemed to be important and which merited inclusion in the framework. Their feedback was recorded and incorporated into the framework. Table 6.2 depicts the

constructs and their factors which emerged from the content analysis, the input of the security professionals which was gathered during the survey and the feedback from the expert reviewers.

Table 6.2: Refined proposed framework constructs

Framework construct	Source	Factors identified
Risk assessment	Content analysis	Assets identification
		Vulnerability and threats assessment
		Risk identification
		Legislation
	Survey	Risk appetite
		Evaluating existing security measures
	Expert review	Risk assessment documentation
Information security policy construction	Content analysis	High level security policy
		Detailed security policy
		Lower level security policy
		Consultation of Stakeholders'
Information security policy implementation	Content analysis	Information security policy awareness
		Information security policy training
		Role of stakeholders
		Information security policy education
Information security policy monitoring and assessment	Content analysis	Non periodic review
		Automated review
		Review of the audit information
		Periodic review
Information security policy compliance	Content analysis	Attitude
		Social pressure
		Benefit of compliance
		Knowledge
Management support	Content analysis	Policy approval
		Management leadership
		Management involvement
		Budget
Employee support	Content analysis	Deterrence measure
		Binding agreement
		Job termination
		Employee involvement
Stakeholders support	Survey	Human resources
		Security specialists
		Clients stakeholders
	Expert review	Legal team
International security standards	Survey	Standards
Guidelines	Expert review	Guidelines

In the section below each of the constructs presented in Table 6.2 is discussed together with the factors identified.

6.4.1 Risk assessment construct

As depicted in Figure 6.3 the risk assessment construct is composed of seven factors.

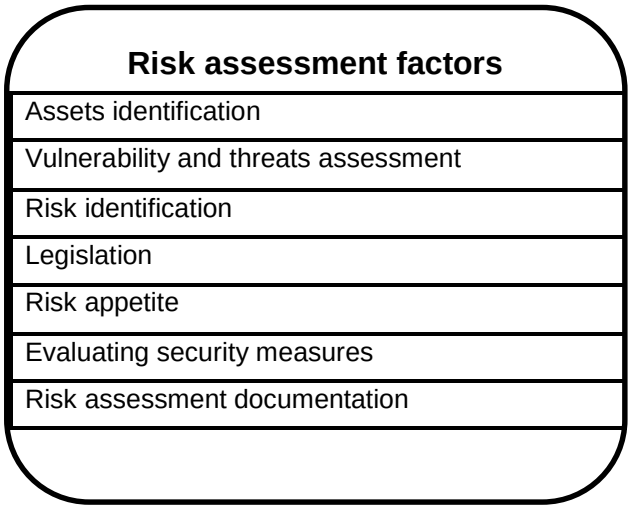


Figure 6.3: Risk assessment factors

Each of the seven factors of risk assessment shown in Figure 6.3 is briefly discussed in the following sections.

6.4.1.1 Identification of assets to be protected

Before the risk process commences it is important to first identify the assets that the organisation needs to protect (Kadam, 2007). NIST SP 800-30 (2011) highlights the need to collect system-related information such as information on the hardware, software, system interfaces (e.g. internal and external connectivity) and, more importantly, the information which the organisation needs to protect. According to Anand (2012), asset identification is important because it helps to quantify the need to address the threats. The output of this step produces information related to both system description and data identification such as system boundary, system functions, system and data criticality and system and data sensitivity (NIST SP 800-30, 2011). The next step involves listing all the threats that may cause harm to the assets which have been identified.

6.4.1.2 Identification of threats and vulnerabilities

The Information technology - Security techniques - Systems Security Engineering - Capability Maturity Model: ISO/IEC 21827 (2008, p. 9) defines *threats* as "capabilities, intentions and attack methods of adversaries, or any circumstance or event, whether originating externally or internally, that has the potential to cause harm to information or to a program or system, or to cause these to harm others." NIST 800-30 Risk Management Guide for Information Technology Systems (2011) identified the following as the sources of threat to an organisation's information: hackers, crackers, computer criminals, terrorists, industrial espionage, and insiders (poorly trained, disgruntled, malicious, and negligent or terminated employees). The output of the threat identification is the threat statement which contains the list of potential threat-sources that may jeopardise the organisation's information (NIST 800-30, 2011). This information helps to determine the likelihood of a threat exploiting system vulnerability.

NIST 800-30 (2011, p. 7) defines a *vulnerability* as "a flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy." NIST 800-30 (2012) observes that the primary objective of vulnerability assessments is to understand the nature and degree to which organisations, business processes, and information systems are vulnerable to threat sources. Thus, vulnerabilities are recognised deficiencies in the information assets which may be exploited by the threats and, therefore, causes harm to such information. Information may have multiple vulnerabilities, for example, an organisational database which has weak access control, poor backup procedures and/or system identifiers of terminated employees (ID) and which have not been removed from the system (NIST 800-30, 2011). The result of this step is a list of system vulnerabilities (flaws or weaknesses) that may be exploited by the potential threat-sources which were identified during the threat identification.

6.4.1.3 Legislation identification

The main reason for developing an information security policy is to mitigate the various security risks that organisations face. One such risk is the proliferation of regulatory requirements (Doherty et al., 2009). Weil (2003); Edwards (2011) and Avolio et al. (2007) argue that it is imperative that organisations first identify and understand all the regulatory requirements that dictate the creation of such policies before writing an information security policy. Avolio et al. (2007) suggest that information security policy developers

should familiarise themselves with the penalties of non-compliance with relevant laws as this will assist the organisations to prioritise their policies and implement the proper level of discipline in respect of employees who violate policies. Kadam (2007) maintains that information security policies are important controls because they help the organisation to comply with legislation by mapping the policy statements to legislative requirements.

6.4.1.4 Risk identification

Felton (2010, p. 5) states that "the goal of risk identification is to separate acceptable minor risks from potentially catastrophic risks as well as provide enough information to analyse and mitigate the entire risk portfolio." NIST 800-30 (2012) suggests that the risk identification step involves assessing the level of risk in terms of the likelihood of a given threat-source attempting to exploit a given vulnerability and conducting an impact analysis.

Likelihood determination

The objective of the likelihood determination is to ascertain the probability rating should a potential vulnerability be exploited. As shown in Table 6.3 the likelihood that a potential vulnerability could be exploited by a given threat-source may be described as high, medium or low (NIST 800-30, 2011).

Table 6.3: Likelihood definition

Likelihood level	Likelihood definition
High	The threat-source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective.
Medium	The threat-source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability.
Low	The threat-source lacks motivation or capability, or controls are in place to prevent the vulnerability from being exercised.

The output of this step produces an overall likelihood rating (high, medium, low) that indicates the probability that a potential vulnerability may be exploited. Once this step has been completed, the next step involves the impact analysis.

Impact analysis

NIST 800-30 (2012, p. 8) defines impact as follows: "the level of impact from a threat event is the magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system

availability." The impact (consequence) is analysed in terms of the organisation's loss of integrity, availability and confidentiality (NIST 800-30, 2012). The output of the impact analysis is an impact rating (high, medium, or low) which specifies how critical the impact would be if the threat exploits the vulnerability.

6.4.1.5 Risk appetite

This factor was added based on the comments of the security professionals who participated in the survey. One security professional suggested that "It is important that organisations specify their risk appetite or what risks are they willing to accept." Although an organisation may be prepared to take the risk, Douglas (2011) recommends that the risk appetite be measured and quantified. Douglas (2011, p. 15) goes on to say that: "the risk appetite statement is generally considered the hardest part of any enterprise risk management implementation. However, without clearly defined, measurable tolerances, the whole risk cycle of any risk framework is, arguably, at a halt."

6.4.1.6 Evaluating existing security measures

This factor was added based on the comments made of security professionals who participated in the survey. One security professional stated that: "once a risk has been identified, there is a need to evaluate existing security measures to see if they can mitigate the risk or new security measures are needed to encounter the threats." The output of this step comprises the recommendation of controls and alternative solutions in order to mitigate the risk (NIST 800-30, 2011). The controls may be either technical controls such as the installation of anti-virus software or non-technical controls, for example, an information security policy may be selected as the main control as regards mitigating the risk of insider employees who negligently put an organisation's information assets at risk. It is vital that the recommended controls either eliminate or reduce the risk to an acceptable level. The final step in the risk assessment process is the risk assessment documentation.

6.4.1.7 Risk assessment documentation

Once the risk assessment processes have been accomplished, the output of each of the processes of the risk assessment should be documented in an official report. These outputs include threat-sources, vulnerabilities identified, risks assessed and recommended controls for mitigating the risks. The risk assessment report produced will assist top management to understand the risks associated with an organisation's assets

and to allocate resources such as the budget to reduce the risk to an acceptable level (NIST 800-30, 2011). Once the risk assessment process has been completed, the next step involves the formulation of the information security policy.

6.4.2 Information security policy construction construct

As depicted in Figure 6.4 the information security policy construction construct is composed of four factors.

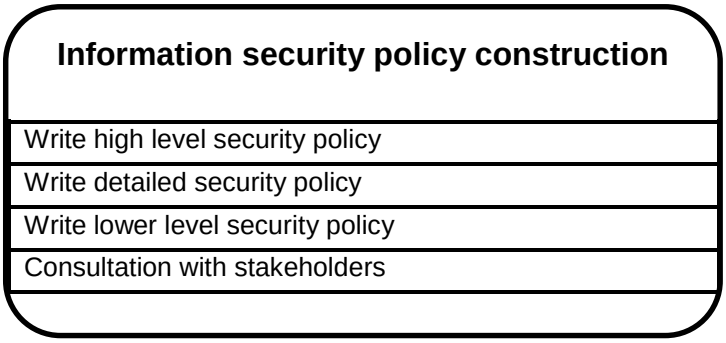


Figure 6.4: Information security policy construction factors

This research project follows the recommendation of the Mauritian Computer Emergency Response Team (2011) with regard to the development of information security policies as this recommendation provides a comprehensive methodology with which to constructing a security policy. The Mauritian Computer Emergency Response Team (2011) suggests that an information security policy should be constructed based on the employees' roles in the organisation. Employees all have different roles in an organisation and they are likely to look for different things from an information security policy perspective. For example, although an executive manager is not that interested in the technicalities of implementing the security guidelines of the network firewall, this is the main focus of technical staff. Thus, if it is borne in mind that the various employees in an organisation require different types of information security policies, it becomes critical that the development of such security policies should take into account this requirement. Figure 6.5 depicts the Mauritian Computer Emergency Response Team's (2011) proposed hierarchical policy structure which is divided in 3 categories, namely, governing policy, technical policy and guidelines.

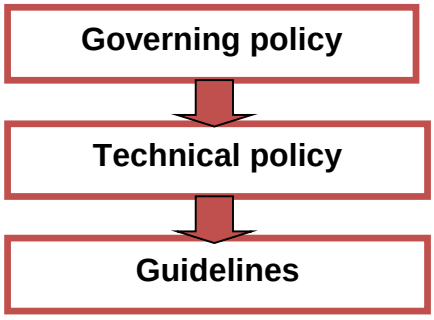


Figure 6.5: Policy hierarchy

As discussed in Chapter 3, Governing policies are referred in this study as high level security policies because they are implemented at the top management level. Technical policies are termed detailed security policy because they provide detailed processes of the implementation of the high level security policies while guidelines are referred as lower level security policies because they are implemented at the operational level of the organisation.

6.4.2.1 Writing high level security policy

The Mauritian Computer Emergency Response Team (2011) emphasises that the governing policy should address information security at a high level. Governing policies are written by executive management. Executive management, which is in control of the organisation as a whole, is responsible for issuing high level mandates which comprise information to be used by security professionals while developing security policies (Bayuk, 2009). These high level security policies are dealt with by managers in order to gain a sense of the company's overall security policy philosophy (Diver, 2007). Governing policies are supported by technical policies which provide detailed statements on compliance with the governing policies (Mauritian Computer Emergency Response Team, 2011).

6.4.2.2 Writing detailed security policy

The Mauritian Computer Emergency Response Team (2011) points out that the technical security policies are implemented by the technical staff as they perform their daily activities. Von Solms et al. (2011) referred to technical security policy as tactical security policy. These policies are the instructions manual for how an organisation's assets should be secured. Examples of detailed security policies include the following: internet usage policy, email usage policy, network security policy, security of operating system policy, etc. In other words, detailed security policies describe what must be done but not

how to do it as the latter is reserved for the guidelines (Mauritian Computer Emergency Response Team, 2011).

6.4.2.3 Writing lower level security policy

Lower level security policies are written for the employees at the lower levels. These lower level security policies are the more detailed descriptions of the way in which to accomplish a specific task in order to comply with a specific information security policy requirement. Lower level security policies contain a documentation of the technical standards that guide lower level employees on how to comply with the information security policy (Von Solms et al., 2011). Lower level security policies include for example, procedures to follow when configuring and maintaining network firewall.

Once the initial information security policy has been developed, it is essential that such documents go through a review cycle process before they are finally approved by top management. The next section discusses the review and approval processes.

6.4.2.4 Consultation with stakeholders

Bonehill (2007) emphasises that, once an information security policy draft has been agreed upon by the policy sponsors, it must go through the consultation stage before it is submitted to senior management for approval. According to Diver (2007), the information security policy should be reviewed by any groups who would be expected to work with such policy. In addition, it is important to involve those individuals/groups who will be responsible for ensuring that the information security policy is both enforceable and effective. Griffins (2009) proposes that the security policy should be reviewed by groups of people who have knowledge about security policy development and who understand the mechanisms of enforcing a security policy. Such groups include existing policy users, system administrators (Diver, 2007) as well as the legal and internal audit departments (Talbot and Woodward, 2009). Figure 6.6 presents a flow chart diagram summarising the discussion on the processes involved in constructing an information security policy.

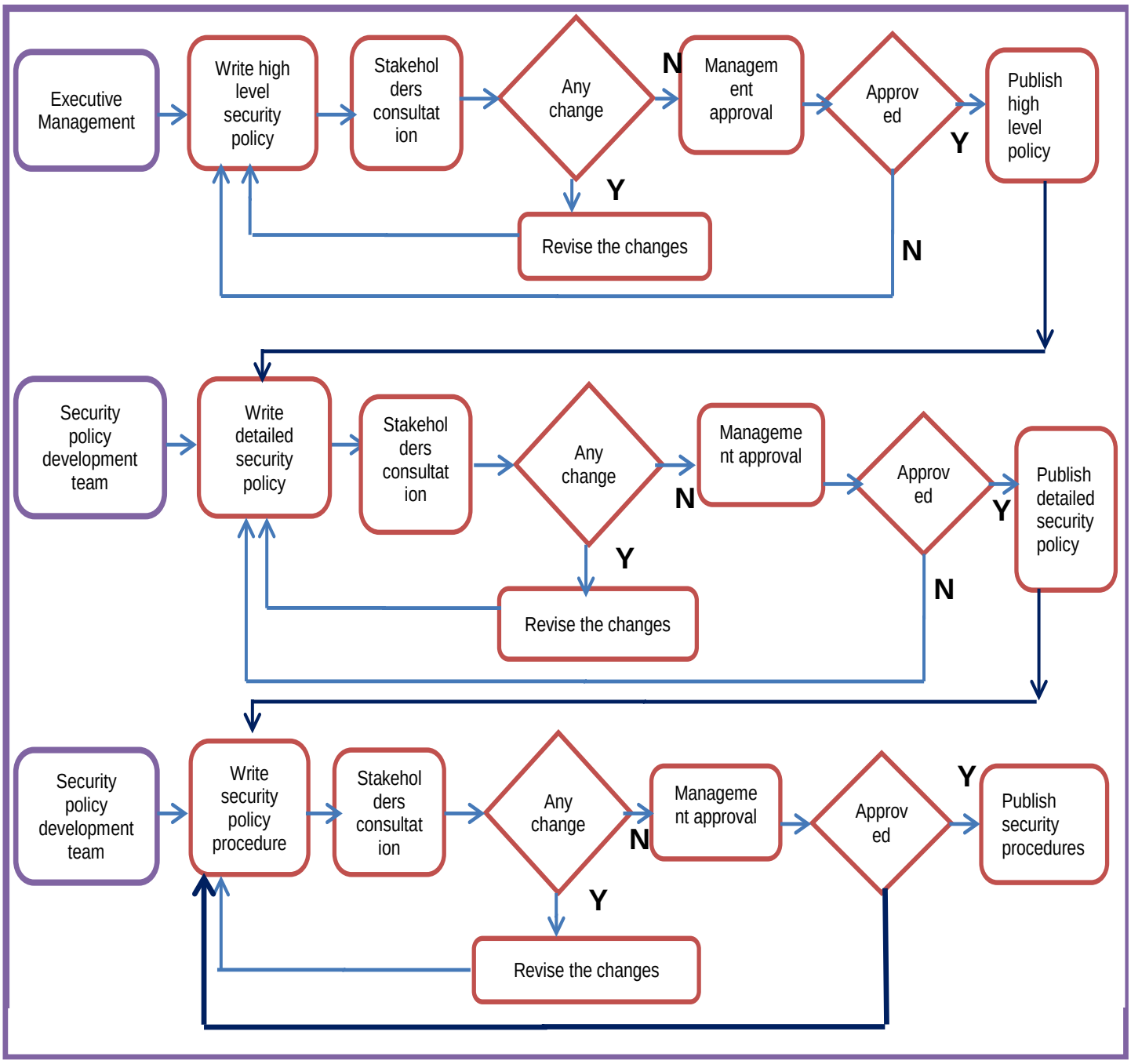


Figure 6.6: Flow chart diagram of information security policy construction

Once the information security policy construction has been completed, the next stage involves the implementation of the policy across all the levels of the organisation.

6.4.3 Information security policy implementation construct

As presented in Figure 6.7 the information security policy implementation construct is composed of four factors.

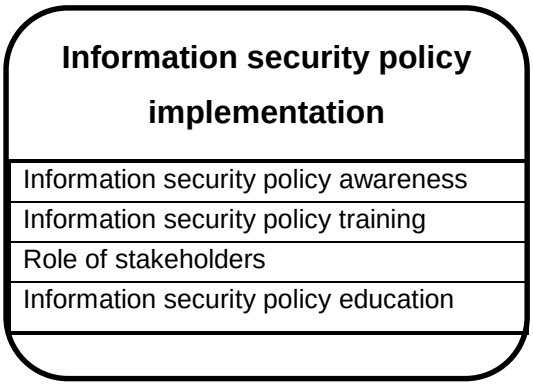


Figure 6.7: Information security policy implementation factors

The most difficult part of the information security policy development process is rolling it out to the organisation (Kadam, 2007; InstantSecurityPolicy, 2013). Johnson and Merkow (2010) maintain that "the process of implementing security policies can be harder than creating the document itself." The introduction of a new information security policy will bring about changes in the way in which employees behave in their handling of the organisation's information. It is essential to obtain support of the organisation's community in accepting the new changes.

According to Johnson and Merkow (2010, p. 112), "implementing security policies successfully takes a combination of soft skills in dealing with human nature and company culture and hard skills in project management." Thus, the challenge is to convince the employees about the need for the new information security policy requirements so that it becomes an integral part of their daily security practice. This may be achieved by educating and training employees on the new information security policy requirements.

6.4.3.1 Information security policy awareness

Once an information security policy has been created and implemented throughout the organisation, it is crucial that the employees who are involved in adopting and complying with the information security policy are made aware of the new security policy requirements. "Failing to make users aware of a policy can lead to a decrease in security through user behaviour that does not comply with policy, be intentional or not" (Talbot and Woodward, 2009, p. 9).

It is, thus, imperative that there be a communication plan in place to ensure that the security policy is communicated to all the stakeholders (departmental executives, business managers, legal team, human resources and internal audit team) in the

organisation (D'Arcy et al., 2009). The objective of information security awareness is to ensure that all the stakeholders are aware of and understand their responsibilities in respect of the security policy requirements. Thus, in order to reach this audience, various business communications (notices, intranet, posters, newsletters, etc.) may be used to promote security policy awareness. While Furnell (2010) recognises the importance of security awareness, he does point out that security awareness is not always sufficient to improve the security behaviour of employees. Accordingly, organisations need to use mechanisms such as information security training and education to support the security awareness approach. The next sections discuss the role of information security policy training and education.

6.4.3.2 Information security policy training

The acceptance of an information security policy within the entire organisation depends on numerous factors, including the conflicting demands of security versus ease of use (Kadam, 2007; Johnson and Merkow, 2010). Kadam (2007) maintains that "human ingenuity will always find ways of circumventing things which are viewed as obstacles." It is, thus essential that employees do not consider the information security policy as a hindrance to their daily operations but rather as a tool that will help the organisation to realise both its objectives and mission. Therefore, in order to facilitate the acceptance of the information security policy acceptance, organisations need to train their employees in the new policy requirements.

Diver (2007) discusses that, despite the fact that organisations conduct training sessions, employees may choose to ignore such policy training. In order to solve this problem, Diver (2007) proposes that the organisation should institute a contractual requirement to attend the policy training. Employees will also be required to sign that they have attended the training. Rezgui and Marks (2008) maintain that the information security training programme should inform employees about the organisation's information security policies and also make them aware of the risks and potential losses to which the organisation may be exposed should the employees not adhere to such security policies.

6.4.3.3 Information security policy education

Information security researchers agree that a Security Education, Training, and Awareness (SETA) programme is essential as security education, training and awareness are three important pillars that are crucial in controlling information security misuse (D'Arcy et al., 2009; Whitman, 2004; Thomson and Von Solms, 2006). According to

D'Arcy et al. (2009), a SETA program extends beyond just awareness of security policy and often includes ongoing efforts to (1) convey knowledge about information risks in the organisational environment, (2) emphasize recent actions against employees for security policy violations, and (3) raise employees' awareness of their responsibilities regarding organisational information resources.

NIST SP 800-16 (2013, p. 45) differentiates between awareness and training as follows:

> "Awareness is not training. The purpose of awareness presentations is simply to focus attention on security. Awareness presentations are intended to allow individuals to recognise IT security concerns and respond accordingly. In awareness activities, the learner is the recipient of information, whereas the learner in a training environment has a more active role. Awareness relies on reaching broad audiences with attractive packaging techniques. Training is more formal, having a goal of building knowledge and skills to facilitate the job performance."

Thomson and Von Solms (2006) maintain that the objective of an information security awareness programme is to focus the employees' attention on information security while the information security training programme should reinforce the content of information security awareness programme while giving employees the opportunity to apply their learning through hands-on activities. It may be argued that it is not possible for security awareness and learning to happen in "one hit" but that a learning curve is a necessity.

Thomson and Von Solms (2006) proposed an Information Security Competence Maturity Model. In terms of this model, the Conscious Competence Learning Matrix is generic and may cover a wide variety of skills. At Stage 1 employees are at the unconscious, incompetent stage. This, in turn, implies that they are not aware of what is to be done in terms of information security and are also not aware of their own ineffectiveness. If employees are to advance from Stage 1 to Stage 2, the organisation must implement an effective information security awareness and training programme. Through security awareness, training and experience, the ideal objective of the Information Security Competence Maturity Model is for the employees in an organisation to reach Stage 4 and become unconsciously competent in practising information security (Shayan, Soheili, and Abdi, 2009). Figure 6.8 depicts the progression of employees' security awareness, training and experience from unconscious incompetence to information security obedience.

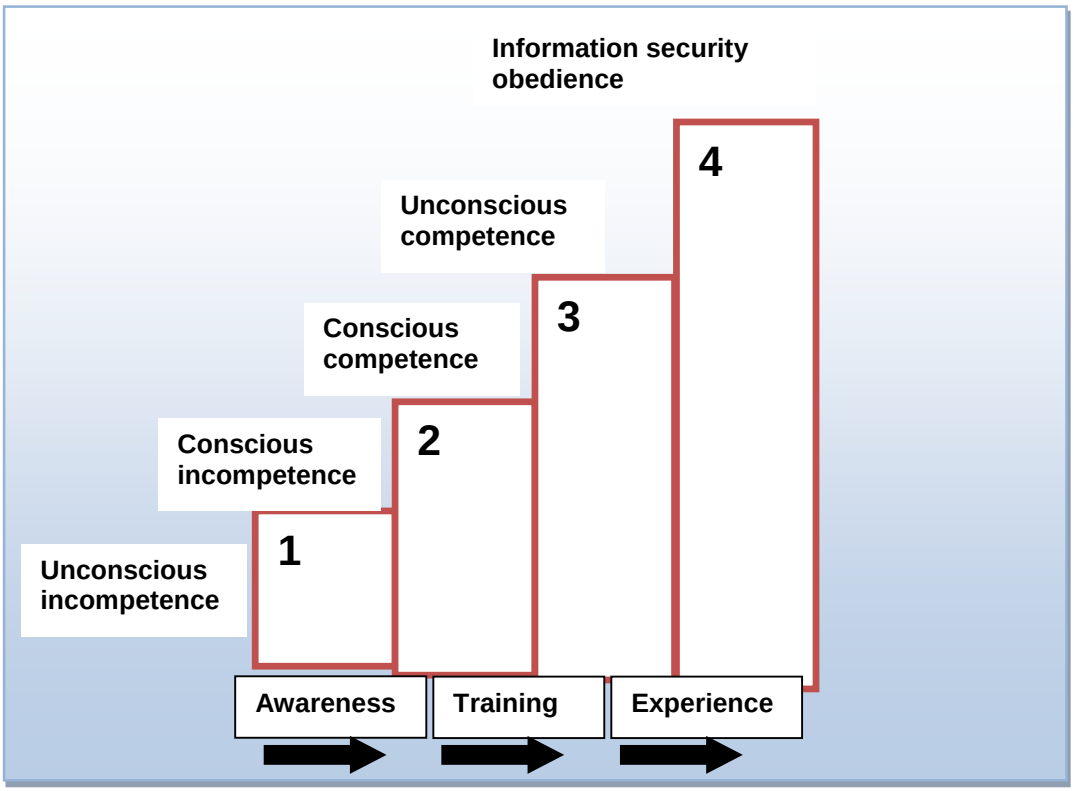


Figure 6.8: Information Security Competence Maturity Model (Thomson and Von Solms, 2006)

This Information Security Competence Maturity Model proposed by Thomson and Von Solms (2006) is crucial to information security policy training, awareness and education as employees are expected to learn lengthy policies, guidelines and procedures. This is not a task that may be accomplished in one day. When the security policy is first introduced in the organisation, employees are usually completely unaware of the requirements of the policy. However, after several training and education sessions, the employees will be aware of and comfortable with the policies and this, in turn, will result in security practices within the organisation.

6.4.3.4 Roles and responsibilities of stakeholders

Both Diver (2007) and Bayuk (2009) highlight the importance of assigning roles and responsibilities during the implementation of information security policies. Various departments may be assigned different job descriptions, for example, the technology development department may be tasked with checking security vulnerabilities while HR departments may be asked to record lists of current employees and contractors (Bayuk, 2009). Wood (2011) argues that if the responsibility for information security training and awareness is not assigned and documented, it is likely that this task will not be

accomplished because it will not be anyone's responsibility to ensure that such training is done.

Once the information security policy has been implemented within the organisation and all employees have been trained and educated in the new information security policy requirements, it is important that organisations implement appropriate monitoring mechanisms to define the daily activities throughout the organisation.

6.4.4 Information security policy monitoring and review construct

As depicted in Figure 6.9 the information security policy monitoring and review construct is composed of 4 factors.

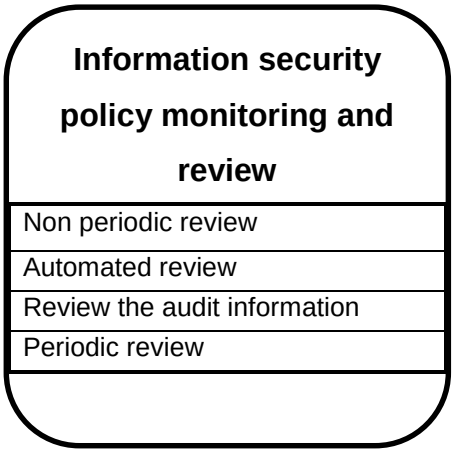


Figure 6.9: Information security policy monitoring and review factors

The need to review and update the security policy either periodically or non-periodically is essential in an organisation (Talbot and Woodward, 2009). Chuvakin (2008) and Talbot and Woodward (2009) claim that, if the information security policy is not reviewed and updated, this may result in the organisation not addressing risks to its information resources. The Mauritian Computer Emergency Response Team (2011) states that the information security policy review and assessment should be conducted if there is a valid reason for this process to take place, such as changes in the information systems or an emergence of new threats. Such changes may encompass, for example, new legal requirements and drastic technological changes. However, Diver (2007) recommends that there be a balance of good security practices and the result of the review process. For example, Diver (2007, p. 25) states that "from a due diligence viewpoint, it is not acceptable to change good policy to inadequate policy just because there were a number of requests to deviate from that policy by certain groups within the company."

6.4.4.1 Periodic review of information security policy

Hong (2006) suggests that the information security policy should be evaluated and reviewed on a regular basis to ensure sure that the latest threats, new regulations and government policies are addressed. In addition, Diver (2007) proposes that security policy should be reviewed annually to ensure that the policy does not become outdated as a result of changes or implementation of new technology. Talbot and Woodward (2009) claim that a reason to review the information security policy may be based on the deployment of new technology such as happens when old software or hardware is decommissioned.

6.4.4.2 Non-periodic review of information security policy

Hong et al. (2006) and Diver (2007) agree on the necessity of both a periodic review and non-periodic review of the information security policy. According to Hong et al. (2006), periodic evaluation is the assessment of the security policy as specified in the policy, while a non-periodic review is conducted in the event of serious security accidents, organisational transformation and drastic technology change (Osborne, 1998; Hong et al., 2006). Diver (2007) supports this notion by adding that ad hoc updates are necessary when fundamental changes in technology render the existing policy processes either fully or partially redundant.

6.4.4.3 Review of audit information

As regards monitoring the information security policy throughout the organisation, the Generally Accepted Principles and Practices for Securing Information Technology Systems NIST SP 800-14 (1996, p. 50) states that “audit trails maintain a record of system activity by system or application processes and by user activity. In conjunction with appropriate tools and procedures, audit trails can provide a means to help accomplish several security-related objectives, including individual accountability, reconstruction of events, intrusion detection, and problem identification.”

Audit trail log files should be examined on a regular basis by security personnel in order to find out whether any unauthorised activities have taken place (RSA Security Inc, 2009). An audit trail contains sufficient information to identify the events that have occurred and who (or what) caused such events (NIST SP 800-14, 1996).

6.4.4.4 Automated review of information security policy

In order to facilitate the security policy review and maintenance, Talbot and Woodward (2009) advise the use of an automated system of review scheduling which timeously alerts when a major change to the existing security practices has occurred. The International Standards of Supreme Audit Institutions (ISSAI 5310, 1995) highlights the importance of using automated software so as to minimise the time and effort users spend in accomplishing their tasks. "By using automated technology, the users are not significantly relying on computer applications but are achieving noticeable efficiencies" (ISSAI 5310, 1995, p. 24).

Security violations, policy deviations, and audit information should also be reviewed (Diver, 2007) as this helps to identify any areas in which policy has not been enforced or frequent policy deviations have occurred. Once the information security policy has been implemented in the organisation, it is crucial to put mechanisms in place that will ensure both compliance with and enforcement of such new information security policy.

6.4.5 Information security policy compliance construct

As depicted in Figure 6.10, the information security policy compliance construct encompasses four factors.

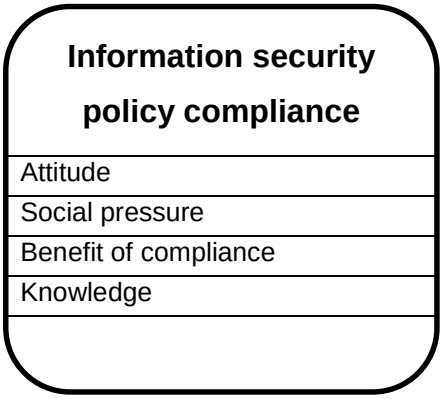


Figure 6.10: Information security policy compliance factors

As stated in Chapter 3, this study is grounded on existing theories related to information security policy such as the Theory of Planned Behaviour (TPB). Based on TPB, Bulgurcu et al. (2010) argue that an employee's intention to comply with the organisation's information security policy is related to the employee's attitude to compliance, normative

beliefs and perceived behavioural control. Figure 6.11 presents the antecedents of information security policy compliance.

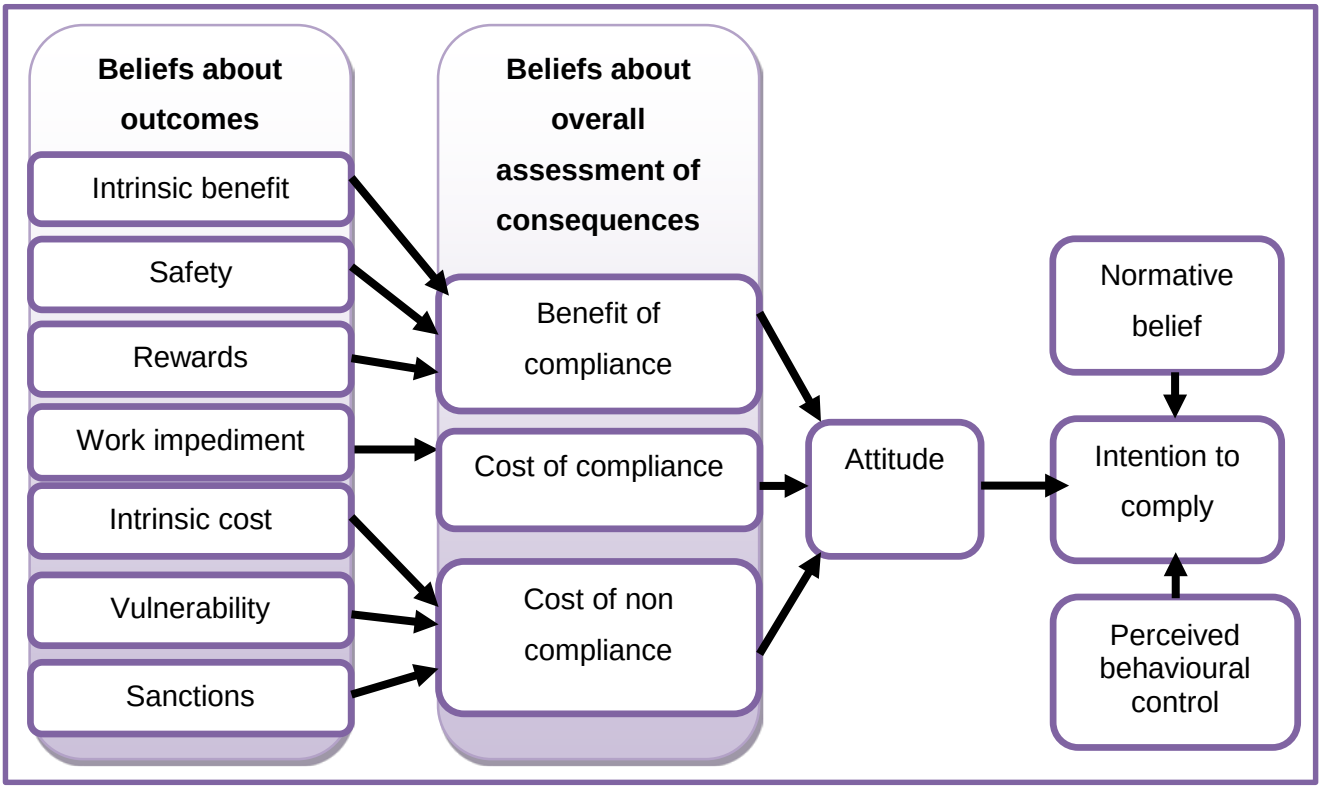


Figure 6.11: A proposed model of the antecedents of information security policy compliance (Bulgurcu et al., 2010)

The following section briefly discusses the findings of the proposed model of Bulgurcu et al. (2010).

6.4.5.1 Attitude

The literature clearly highlights that an employee's attitude to carrying out a certain behaviour is determined by the employee's evaluation of his/her beliefs regarding the consequences of performing such behaviour (Ajzen, 1991; Fishbein 2007; Fishbein and Ajzen, 1975). Bulgurcu et al. (2010, p. 6) state that "an employee's positive attitude towards compliance with the organisation's information security policy positively influences his/her intention to comply with the requirements of the information security policy." In addition, Bulgurcu et al. (2010) found that an employee's beliefs about the overall assessment of possible consequences would influence the employee's attitude to compliance with the information security policy requirements. They argue that, if an employee believes that the effort involved in complying with the information security policy is less important, then he/she is likely to comply with the policy.

6.4.5.2 Knowledge

Bulgurcu et al. (2010) suggest that information security policy awareness is important in order to enhance the employee's knowledge of the information security policy requirements. They found that "an employee's judgment of his/her own knowledge in complying with the requirements of the information security policy positively influences his/her intention to comply with the requirements of the information security policy." Employees who have undergone information security policy awareness will have acquired knowledge about both the benefits and disadvantages of compliance with the requirements of the information security policy.

6.4.5.3 Normative beliefs: perceived social pressure

Perceived social pressure refers to a person's perception of what people who are important to that person think about a given behaviour (Fishbein and Ajzen, 1967). Chan et al. (2005) claim that employees tend to comply with the information security policies if they realise that their colleagues, including their peers, supervisors and managers, are complying with such security policy requirements. Bulgurcu et al. (2010) maintain that: "an employee's perceived social pressure about his/her compliance with the requirements of the information security policy positively influences his/her intention to comply with the requirements of the information security policy."

6.4.5.4 Perceived behavioural control: perceived benefit

Perceived behavioural control refers to a person's perceived ease or difficulty as regards performing certain behaviour (Ifinedo, 2012). A study conducted by Lee and Larsen (2009, p. 12) found that "individuals are reticent to follow or adopt recommended responses if they perceive that a considerable amount of resources i.e. time, effort and money will be expected toward effort of such responses." Bulgurcu et al. (2010, p. 8) highlight that "an employee's perceived benefit of compliance with the organisation's information security policy positively influences his/her attitude towards complying with the requirements of the information security policy."

This study supports the proposed model of Bulgurcu et al. (2010) because the model provides a detailed understanding of the factors that clarify the employees' intention to comply with the requirements of the information security policy. In addition, the fact that the model was empirically tested increases the credibility of the contribution made by the model. Hence, this study states that an employee's intention to comply with an

organisation's information security policy is related to the employee's attitude toward compliance, normative beliefs, and perceived behavioural control. The next section discusses the management support construct.

6.4.6 Management support construct

As depicted in Figure 6.12 the management construct encompasses four factors.

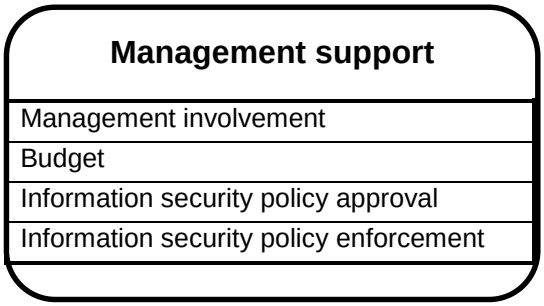


Figure 6.12: Management support factors

Each of the four factors is discussed in the section below:

6.4.6.1 Management involvement

Bayuk (2009) argues that the first step in formulating a security policy involves ascertaining top management's opinions as to how top management understands security in the organisation. "The implementation of security policy must start from the executive management" (Bayuk, 2009, p. 1). The involvement of executive management in the information security policy development is a key factor in the successful development and implementation of security policies (Kadam, 2007; Maynard et al., 2011). Management plays a significant role in the decision making in an organisation. Kadam (2007) highlights that it is essential that management is informed about the importance of information security policy development activities so that the necessary resources may be allocated.

6.4.6.2 Budget

As discussed in Chapter 3, the process of developing and implementing information security policies require organisations to have a budget in place. The costs of such development and implementation include, for example, the costs involved in reviewing regulatory changes; reviewing new technologies; reviewing major incidents; writing new policies and mapping to frameworks (Lineman, 2009). It is incumbent on management, as the decision maker in an organisation, to ensure that sufficient budget has been voted to cover the costs of developing such policies. Al-Awadi and Renaud (2007) maintain

that “the budget needs to be adequate: without enough money, we can’t have security in the organisation; money will bring software, hardware, and consultants."

6.4.6.3 Information security policy approval

Executive management must give its approval of the information security policy developed in the organisation (Kadam, 2007). InstantSecurityPolicy (2013) highlights that an information security policy is an official organisational document and, therefore, it requires management approval. Griffins (2009) proposes that the information security policy should be submitted to a committee tasked with policy approval and composed of various stakeholders. Once the committee has approved the security policy, it is then sent to the top executives and the CEO for final approval.

6.4.6.4 Information security policy enforcement

Johnson and Merkow (2010) maintain that “without executive support, policies are just words. To have meaning, they must be given the right priority and be enforced.” Indeed, top management plays a significant role in the enforcing information security policy and ensuring that employees regard the policy requirements in a serious light. If information security policies are not enforced by top management, employees are likely to neglect them and not follow them. Diver (2007) claims that the participation of senior management in the security policy development is paramount because the security policy is then seen to have “teeth” and this, in turn, helps with both enforcement and compliance throughout the entire organisation.

6.4.7 Employee support construct

As depicted in Figure 6.13 the employee support construct is composed of four factors.

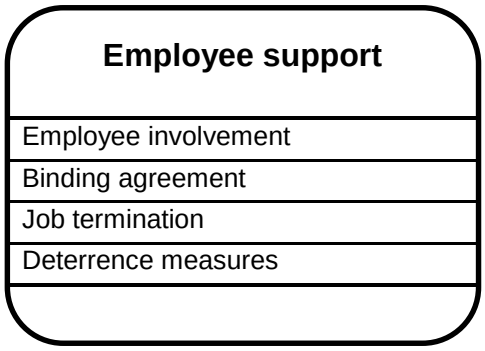


Figure 6.13: Employee support factors

6.4.7.1 Employee involvement

Employee support refers to the support of the end-users who perform various activities in an organisation. Maynard et al. (2011) and Szuba (1998) highlight that involving employees in the development of an information security policy results in their "buy-in" and, thus, employee support while also creating a sense of ownership as regards the information security policy.

Maynard et al. (2011) further recommend that the end-user community is part of the development effort to ensure that the multidisciplinary nature of the organisation is incorporated in the information security policy development process. Diver (2007) suggests that the end-users should be involved in the policy development at an early stage so that they are given the opportunity to identify errors and difficulties which may then be remedied before the security policy implementation. "If the policy documents are hard to understand, users may not read them fully or may fail to understand them correctly, thereby needlessly risking security compromise" (Diver, 2007).

In order to ensure an effective information security policy, it is imperative that everybody in the organisation implement the policy. This, in turn, would ensure the accountability of everyone as regards implementing the policies (Johnson and Merkow, 2010). If employees fulfil the requirements of the information security policy on a day-to-day basis, this would help to create a security culture that would protect the organisation's information.

6.4.7.2 Deterrence measures

Chen and Li (2014) propose a theoretical model that integrates general deterrence theory and social norms theory. They argue that deterrence measures are indispensable for reducing employees' omission behaviours. Information security omission occurs when employees, who are aware of the organisation's security threats and countermeasures, fail to follow such countermeasures. Workman et al. (2008) term this phenomenon the knowing–doing gap. Furthermore, they believe that social norms, such as subjective norms, play a critical role in understanding the employees' omission behaviour. A subjective norm refers to an individual's perception of "what those who are important think he/she should do in a given situation" (Bobek, Hageman, and Kelliher, 2013). The subjective norm factor was discussed in section 6.4.5. However, this section focuses on sanctions as a measure for enforcing compliance with information security policy. Figure 6.14 presents the proposed model of Chen and Li (2014).

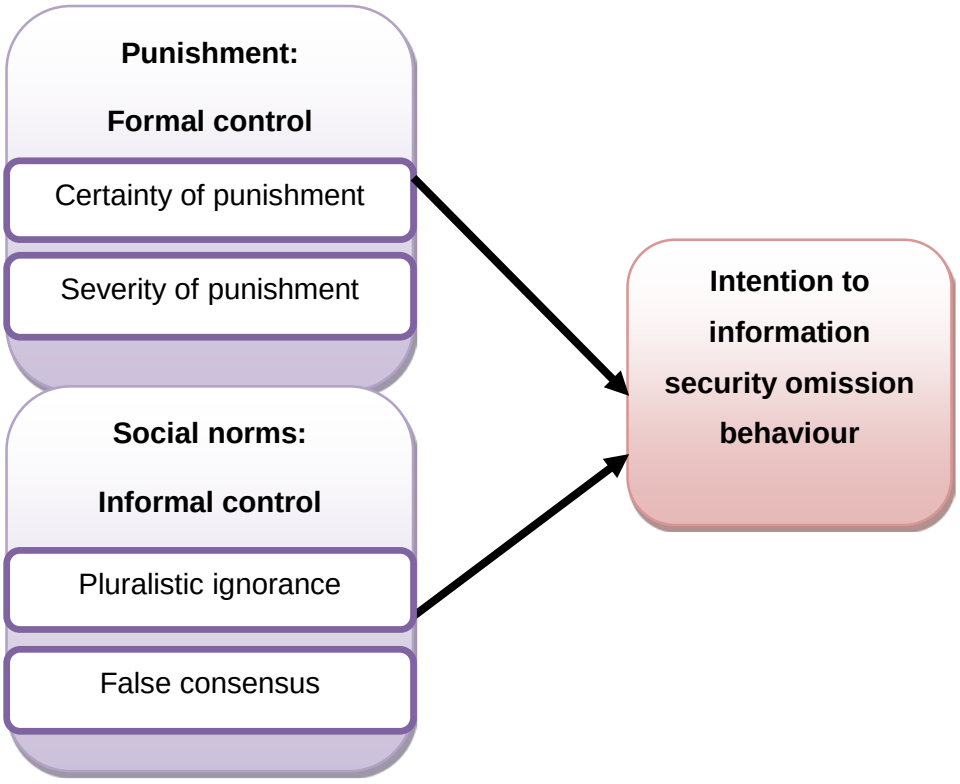


Figure 6.14: Research model (Chen and Li, 2014)

The literature highlights the importance of deterrent measures in reducing inappropriate behaviours on the part of employees (Kankanhalli et al., 2003; Pahnila, Siponen, and Mahmood, 2007; Straub, 1990). Bulgurcu et al. (2010) argue that sanctions are believed to lead to employees perceiving that there is a cost associated with not adhering to security-related rules and regulation. The studies conducted by Pahnila et al. (2007) and Herath and Rao (2009) found that factors rooted in GDT significantly influenced employees' security compliance behaviour. This study argues that deterrence measures reduce the risk of employees intentionally violating the organisation's information security policies. The proposed model of Chen and Li (2014) is a theoretical model. Chapter 7 of this study validate its constructs.

6.4.7.3 Binding agreement

The Businessdictionary (2001) defines a binding agreement as "an agreement in writing between two or more individuals or entities in which a court can impose penalties in the event one party attempts to negate on his or her promise as set forth in the signed document." According to Diver (2007), employees should sign a binding agreement that they will comply with the organisation's policies. The agreement between the employer

and the employee should include information on the sanctions that will be imposed in the event of an information security policy violation.

6.4.7.4 Job termination

Diver (2007) maintains that employees must be given either verbal or written warnings and that disciplinary action should be taken the first time an incidence occurs. However, if the employee continues to carry out the same actions in respect of which he/she was cautioned, then stringent measures should be taken, for example, job termination. The following is an example of a contract agreement regarding internet and email use used by Monarch Bank (2014, p. 14): “any employee using Monarch Bank e-mail is expected to review and follow this policy as well as other applicable Monarch Bank policies. Any violation of these policies or inappropriate or improper use of the internet services or e-mail may result in disciplinary action up to and including termination of employment.”

6.4.8 Stakeholders support construct

The development of an effective security policy requires a combination of the various skills which are the result of the experiences of different stakeholders (Diver, 2007). As discussed in Chapter 7, the respondents in the survey suggested that various stakeholders should be involved in the process of developing and implementing an information security policy. One respondent stated that “the security policy team needs to involve other stakeholders who will be affected by the new security policy. These include, for example, clients”. The literature reveals that there are a number of stakeholders who play a critical role in developing information security policies.

Legal counsel

During the survey one respondent mentioned that: “It is important that the legal team is involved in the information security policy development to ensure that organisations’ policies are in line with government laws.” The legal department is important because it provides information on current laws and anticipated legislative requirements (Diver, 2007).

Technical staff

Technical staff members possess the technical knowledge that the security policy development team may lack. A respondent in the survey (Chapter 7) stated that: “Security specialists must be involved in the security policy development because of their

expertise that might be lacking by the security policy team." The role of security specialists in an organisation pertains to the protection of the organisation's information and, specifically, to the development of security policies (Maynard et al., 2011). Diver (2007) maintains that the information security team should guide the development and revision of each policy document and serve as consultants in respect of security policy development.

However, although the security specialists are familiar with security matters, they may not possess a comprehensive knowledge and understanding of computer systems and communications network systems (Maynard et al., 2011) as this is the role of the ICT specialists. Maynard et al. (2011) claim that ICT specialists are, in most cases, one of the driving forces in information security policy development. In addition to their technological knowledge, ICT specialists should also advise on the level of security that is needed in a specific organisation (Diver, 2007).

Human resources

In order to ensure that security policies are in accordance with the standard organisational practices, it is critical that the human resource department is involved in the security policy development lifecycle (Maynard et al., 2011). Diver (2007) supports this notion by highlighting that the human resource department should review and/or approve the security policy based on how the policy relates to existing organisational policies. This is necessary to ensure consistency between the organisation's security policies and the standard organisational practices (Maynard et al., 2011). Diver (2007, p. 17) supports this notion of consistency by stating that "where the policy touches on topics covered by existing HR policy, e.g., email usage, physical security, you must make sure that both sets of policy say the same thing." In other words, security policies should not contradict human resources policies.

In addition, Maynard et al. (2011) suggest that the human resources department is responsible for ensuring a duty of care by making certain that employees are aware of the information security policy's requirements and that they fully understand how the policy affects them.

External representatives

In addition to the involvement of stakeholders, as discussed in the previous section, Maynard et al. (2011) suggest the need to include external representatives, such as customers, suppliers and other external entities, in the development of security policies.

This is particularly important if the external entities depend on the organisation's computer systems to carry out their activities (Baskerville, 1998; Maynard et al., 2011).

In conclusion, as discussed in this section, the development of an effective security policy requires a combination of the various skills resulting from the experiences of different stakeholders. Although the stakeholders mentioned are all likely to feature in medium to large organisations, Maynard et al. (2011) indicate that, in smaller organisations, individuals would probably be involved in more than one role while some activities may be outsourced. For example, in a small organisation, a single IT manager may fulfil the role of both ICT specialist and security specialist. However, the inclusion of multiple stakeholders in the development of an effective security policy is crucial to an organisation because this gives the organisation as a whole a sense of ownership as regards the security policy and this, in turn, facilitates the security policy acceptance and adoption.

6.4.9 International security standards and best practices

This construct was proposed by the security professional who participated in the survey. They suggested that international standards such as ISO/IEC 27002 are a good starting point in the implementation of information security. The ISO/IEC 27002 (2013) contains crucial information related to information security policy.

Bayuk (2009) supports the notion of using international standards as a baseline framework because they would increase the organisation's stakeholders' trust in the information security policy. Bayuk (2009, p. 5) states that "this is a reasonable approach, as it helps to ensure that that the policy will be accepted as adequate, not only by company management, but also by external auditors and others who may have a stake in the organisation's information security program."

Hong et al. (2006) investigated the role that international security standards play in formulating information security policies. Their findings identified six international standards that are a useful reference when developing an information security policy. These six international standards are presented in Table 6.4.

Table 6.4: International standards for information security policy (Hong et al., 2006)

International Standard	Guidelines
ISO/IEC 27001 (2005)	• "Describe the minimum contents in an information security policy; • Explain what should do with a security policy; • An information security policy should be approved by management; • Published and communicated throughout the organisation; • An information security policy should be evaluated and updated periodically".
BSI IT baseline protection manual	• "Description of drawing up an information security policy; • Coverage topics; • Contents; • Review".
ISACAF (The information system audit and control association and foundation)	• "Describe the process and control needs for implementing an information security policy; • Brief section on the security and internal control; • Framework policy; • Writing and maintaining a document".
GASSP (Generally accepted system security principles)	• "Minimal requirements for an information security policy and principles behind it; • The different processes needed for defining maintaining and implementing the policy; • The hierarchy concept of an information security policy".
GMITS (ISO/IEC PDTR 13335-1)	• "Provide a comprehensive guidance on information security with planning, management and implementation".
ISFs Standard of good practice (The globally representation information security forum, ISF)	• "Performance evaluation; • List the contents of information security policy; • The characteristics of the policy; • Explain the acceptable user behaviour".

As may be seen in Table 6.4, the extent to which the security policy is discussed in the standards varies significantly, with some of the standards concentrating on the content of the policy, and others highlighting the security policy development and implementation requirements. However, there is little doubt that all the characteristics mentioned in these standards may make a definite contribution to the initial knowledge when a security policy is developed.

In addition of the discussion of the nine constructs that make up the refined framework, this chapter also highlights the suggestions regarding the structure of the framework and which emanated from the expert review process discussed in Chapter 10.

6.4.10 Structure of the refined framework

During the expert review process, one expert stated that: “There is a need to have a feedback loop to cater for changes in case some processes have been left out and later need to be added. For example, you are on phase 2 of security policy construction and you notice that some changes need to be done in phase 1 of risk assessment. Every change cannot be described as static.” In order to address this recommendation, arrows that show iterative feedback between constructs are drawn as depicted in Figure 6.16. The next section discusses the dimensions that constitute the refined framework.

6.5 Refined proposed framework

As depicted in Figure 6.15, the refined framework is composed of five dimensions.

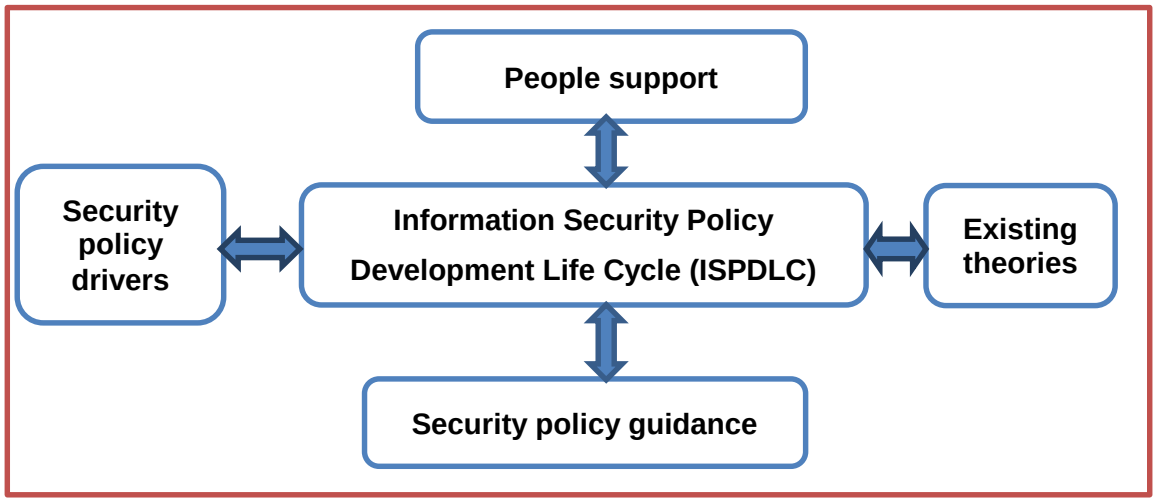


Figure 6.15: Framework dimensions

The first dimension is the **Information Security Policy Development Life Cycle (ISPDLC),** which encompasses the processes needed to develop an information security policy such as risk assessment, policy construction, policy implementation, policy compliance and policy monitoring, assessment and review.

The second dimension is the **security policy drivers**. This dimension is composed of the threats that place the organisation under pressure to put in place mechanisms to protect its information. Abdel-Aziz (2010, p. 7) states that “before discussing information security policy and the process to assess it, it is important to know what drives information security in the first place.” The development of information security policy is driven by both external and internal factors that exert pressure on the organisation to put in place mechanisms to protect the organisation’s information. The internal threats include

employees who place the organisation's information at risk while external threats include hackers, crackers, viruses, etc. In addition, there is the necessity of complying with the proliferating government legislative requirements.

The third dimension is the **security policy guidance**. This dimension is composed of the security standards that guide organisations in constructing an information security policy. As discussed, international security standards such as ISO/IEC 27002 (2013) constitute a major guide at the beginning the information security policy development.

The fourth dimension is labelled the **people support** dimension. This dimension includes all those people who are involved in the development of an information security policy. It is imperative that management, employees and stakeholders support the entire process of developing and implementing an information security policy if it is to survive and attain its objectives.

Finally, organisations need to use relevant **existing theories** in order to understand the behavioural intention of employees as regards information security policy compliance. These dimensions are depicted in Figure 6.16.

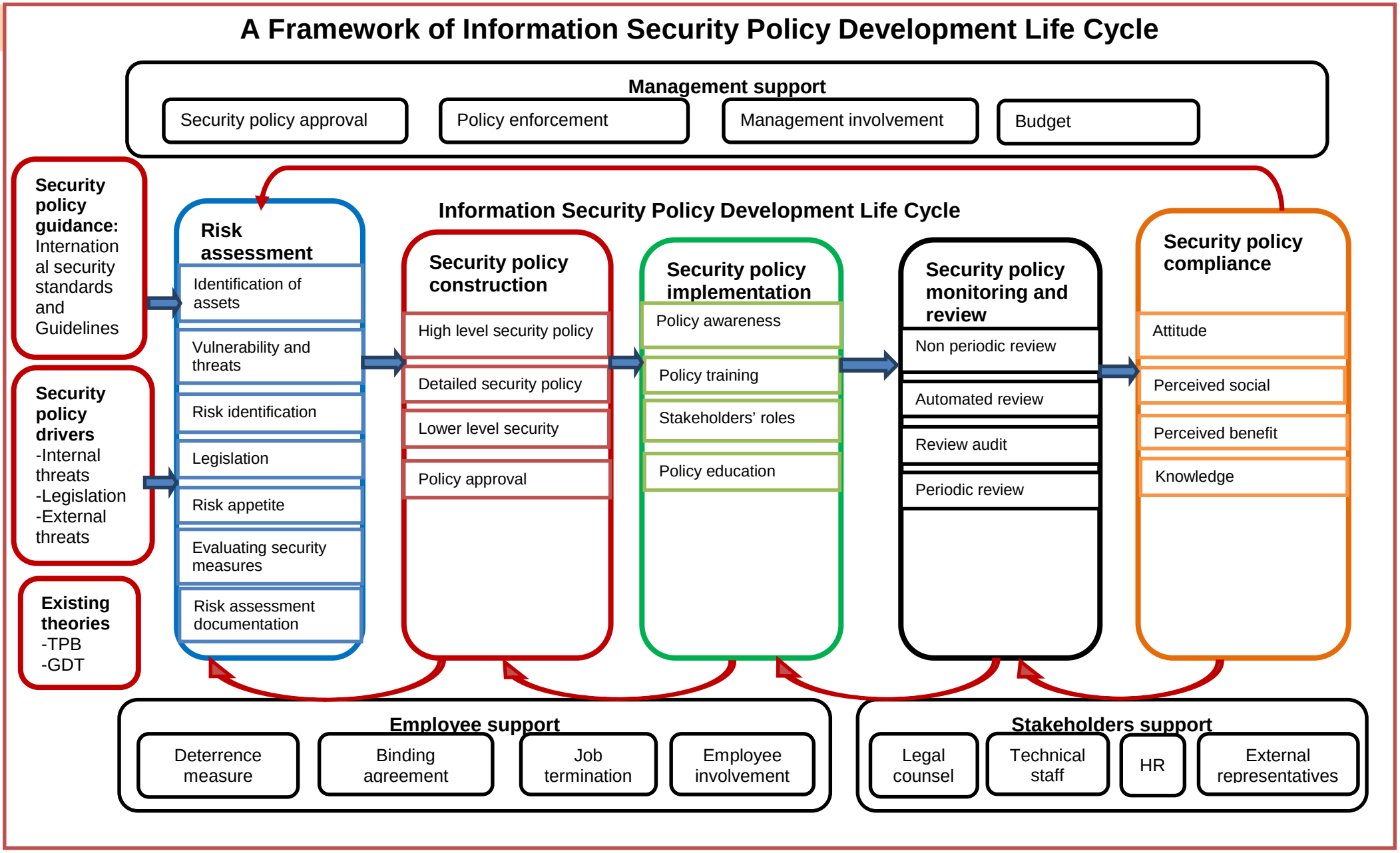


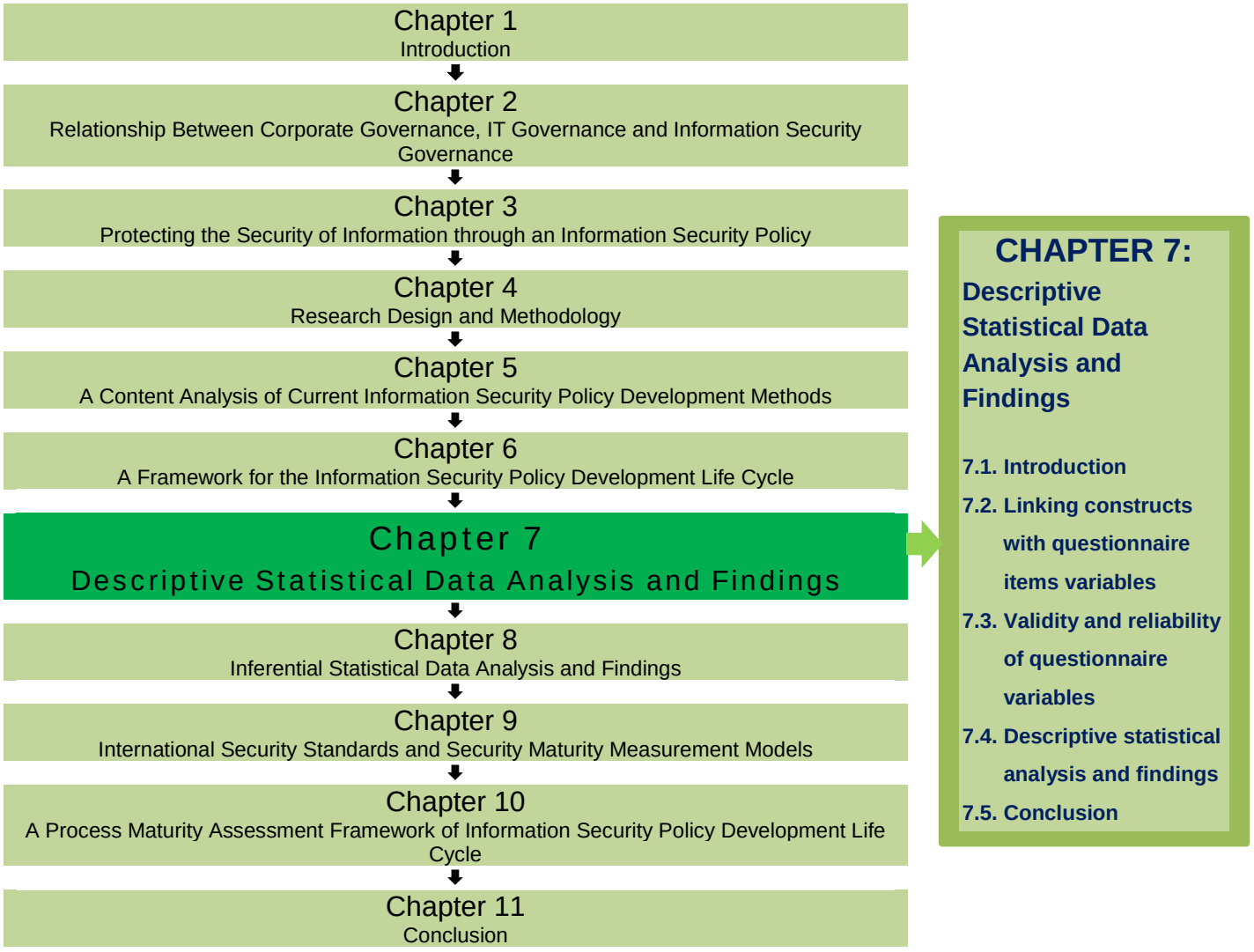
Figure 6.16: A Framework of Information Security Policy Development Life Cycle

6.6 Conclusion

This study posed the following research question: What are the processes that organisations need to follow in developing and implementing an effective information policy. This chapter proposed an information security policy development framework which encompasses the phases that an information security policy should go through its life cycle. The proposed framework includes the constructs that emerged from the content analysis discussed in Chapter 5 and the suggestions of security professionals who participated in the survey and discussed in Chapter 7. In addition, this framework incorporates the feedback provided by expert review as discussed in Chapter 10. The various dimensions suggested by the proposed framework may be regarded as the main pillars of the information security policy development life cycle. The proposed framework ensures both comprehensive and sustainable information security policies.

A focus of this research project was to integrate security maturity assessment into the information security policy development using a maturity model approach. Accordingly, the study investigates current security maturity models in order to ascertain which maturity models would be the most appropriate to use to assess and guide the process of information security policy development. Thus, Chapter 8 investigates the current, available, international standards and security maturity measurement models and their role in assessing the processes involved in information security policy development in order to ensure security quality assurance.

Chapter 7: Descriptive Statistical Data Analysis and Findings



7.1 Introduction

This chapter presents the descriptive statistical data analysis and the findings which emanated from the primary data that was collected during the survey that was conducted. The BusinessDictionary (2004) defines 'statistics' as the "collection, examination, summarization, manipulation, and interpretation of quantitative data to discover its underlying causes, patterns, relationships, and trends." According to Raerd (2011), descriptive statistics organise and summarise data in a meaningful way and one that may be easily interpreted. The main objective of this chapter is to assess the level of importance of the constructs of the framework that was developed and discussed in Chapter 6. The proposed initial framework is composed of seven constructs while each construct includes four factors. The chapter also discusses the importance of the factors.

Firstly, the chapter links the seven constructs of the proposed framework with the questionnaire item variables. Secondly, it discusses the validity and reliability of the construct variables. Cronbach's statistical test was used to measure the reliability and validity of the constructs. Thirdly, the chapter describes the importance of the ISPDLC constructs and their factors. Lastly, this chapter analyses the findings emanating from the qualitative data which was collected via the open ended questions. Table 7.1 summarises the measurement constructs and the objectives of measuring the descriptive statistical data analysis performed in this chapter.

7.1.1 Demographic data collection

The survey targeted a total of 400 security professionals (200 living in the United Kingdom and 200 living in the United States of America). These security professionals were all directly involved with the information security in their organisations and IT managers, Chief Information Officers (CIO), IT security specialists and IT consultants. The respondents were asked to indicate their organisation type, namely, Government, Industrial, Banking, Trading and Education. In addition, respondents were requested to specify the number of employees working in their organisations as less than 500; between 500 and 1000; between 1000 and 5000; 5000 – 10 000; > 10 000.

7.2 Linking constructs with questionnaire item variables

The findings discussed in this chapter emanated from the results gathered from the survey. The questions asked in the survey were subdivided into four categories. The first category aimed to collect the demographic data of the respondents while the second

category was concerned with measuring the level of importance of the seven constructs of the proposed framework. The third category sought to measure the level of importance of the factors of each construct while the last category collected qualitative data with the respondents being asked to suggest any processes that they deemed to be important but which had not been mentioned in the survey.

Table 7.1: Descriptive statistical data analysis objectives

Objective	Measurement construct	Objective of measurement	Questionnaire reference
Investigate the importance of the framework constructs	-Risk assessment -Security policy construction -Security policy implementation -Security policy monitoring -Security policy compliance -Employee support -Management support	Level of importance of the constructs	Q.6 – Q.12
Investigate the importance of the framework constructs sub-variables	-Assets identification -Vulnerability and threats -Risk identification -Legislation	Level of importance risk assessment sub-variables	Q.13 – Q.16
	-Policy audience -High level security policy -Detailed security policy -Lower level security policy	Level of importance security policy construction sub-variables	Q.17 – Q.20
	-Security policy awareness -Security policy training -Role of stakeholders -Security policy education	Level of importance of security policy implementation sub-variables	Q.21 – Q.24
	-Periodic review -Automated review -Audit information -Non periodic review	Level of importance of security policy monitoring and assessment sub-variables	Q.25 – Q.28
	-Policy approval -Policy enforcement -Management involvement -Budget	Level of importance of management support sub-variables	Q.29 – Q.32
	-Deterrence measure -Binding agreement -Job termination -Employee involvement	Level of importance of employee support sub-variables	Q.33 – Q.36
	-Attitude -Perceived social pressure -Perceived benefit -Knowledge	Level of importance of security policy compliance sub-variables	Q.37 – Q.40

7.2.1 Framework construct

A five-point Likert-type scale was used to ascertain the importance of the seven constructs of the proposed framework. The following question was posed to the respondents:

Question: How important do you believe the following factors are for the successful implementation of an information security policy in your organisation? 1) Not important, 2) Somewhat important, 3) Neutral, 4) Important and 5) Very important.

Table 7.2 depicts the measurement constructs and item variables.

Table 7.2: Constructs and measurement variables

Measurement construct	Measurement variable	Item variable
Framework constructs	Risk assessment	A clear understanding of the organisation's security risks.
	Information security policy construction	The information security policy writing process is based on the findings and the recommendations of the risk assessment process.
	Information security policy implementation	Suitable information security policy training and education is conducted during the information security policy implementation stage.
	Information security policy monitoring	Regularly assess and monitor the information security policies to ensure that they are effective.
	Information security policy compliance	Effective information security policy compliance mechanisms to ensure that employees adhere to the organisation's information security policy requirements.
	Employee support	Ensure that employees support and understand their roles and responsibilities as regards the information security policy requirements.
	Management support	Visible support and commitment on the part of the top executive management.

The following section discusses each of the seven constructs shown in Table 7.2.

7.2.2 Risk assessment construct

The questions asked in this category were intended to determine the level of importance of risk assessment processes.

Question: Please indicate the importance of each of the following risk assessment processes 1) Not important, 2) Somewhat important, 3) Neutral, 4) Important and 5) Very important.

The measurement variable and item question variables that compose the risk assessment construct are presented in Table 7.3.

Table 7.3: Risk assessment construct and measurement variables

Measurement construct	Measurement variable	Item variable
Risk Assessment	Assets identification	Develop a risk assessment plan that includes the identification of the assets to be protected.
	Vulnerability and threats identification	Develop a risk assessment plan that includes the assessment of vulnerabilities and security threats.
	Risk identification	Security policy is constructed based on the findings of the risk identification result.
	Legislation	Identify all legislative requirements applicable to the organisations.

The next section discusses the information security policy construction construct.

7.2.3 Information security policy construction construct

The questions asked in this category were intended to determine the level of importance of the information security policy construction processes.

Question: Please indicate the importance of each of the following information security policy construction processes 1) Not important, 2) Somewhat important, 3) Neutral, 4) Important and 5) Very important.

The measurement variable and item question variables that constitute the information security policy construction construct are presented in Table 7.4.

Table 7.4: Information security policy construction construct and measurement variables

Measurement construct	Measurement variable	Item variable
Information security policy construction	Write high level security policy	At the strategic level, develop high level security policies which are a set of management mandates that demonstrate how the executive management plan to protect the organisation's information assets.
	Write detailed security policy	At the tactical level, develop detailed security policies which are detailed statements of the strategic level policies showing what should be done to comply with the security policy.
	Write lower level security policy	At the operational level, develop lower level security policies which define the procedures, plans or processes that address the details of how to perform a specific action.
	Consultation with stakeholders	The organisation's stakeholders must be consulted before the information security policy is submitted to senior management for final approval.

The next section discusses the information security policy implementation construct.

7.2.4 Information security policy implementation construct

The questions asked in this category were intended to determine the level of importance of the information security policy implementation processes.

Question: Please indicate the importance of each of the following information security policy implementation processes 1) Not important, 2) Somewhat important, 3) Neutral, 4) Important and 5) Very important.

The item questions, codes and measurement variables that constitute the information security policy implementation construct are presented in Table 7.5.

Table 7.5: Information security policy implementation construct and measurement variables

Measurement construct	Measurement variable	Item variable
Information security policy implementation	Information security policy awareness	A variety of business communication methods (notices, posters, newsletters, etc.) are used to promote information security policy awareness.
	Information security policy training	There are mechanisms in place to train all stakeholders so that they understand their responsibilities in respect of the security policy requirements.
	Role of stakeholders	Clearly define the roles of the various organisation stakeholders (executive management, information security officials, all employees).
	Information security policy education	There are mechanisms in place to educate employees about the new information security policy requirements.

The next section discusses the information security policy monitoring and review construct.

7.2.5 Information security policy monitoring and review construct

The questions asked in this category were intended to determine the level of importance of the information security policy monitoring and review processes.

Question: Please indicate the importance of each of the following information security policy monitoring processes 1) Not important, 2) Somewhat important, 3) Neutral, 4) Important and 5) Very important.

The item questions and measurement variables that constitute the information security policy monitoring construct are presented in Table 7.6.

Table 7.6: Information security policy monitoring construct and measurement variables

Measurement construct	Measurement variable	Item variable
Information security policy monitoring	Periodic review	Review the information security policy on a regular basis to ensure that the latest threats and new regulations are up-to-date.
	Automated review	Use of automated review scheduling system which alerts when major changes have occurred in existing practices.
	Review of audit information	Review the audit information in order to identify areas of frequent security policy deviation.
	Non periodic review	An established information security policy review and update process exists.

The next section discusses the management support construct.

7.2.6 Management support construct

The questions asked in this category were intended to determine the level of importance of the management support processes.

Question: Please indicate the importance of each of the following management support processes 1) Not important, 2) Somewhat important, 3) Neutral, 4) Important and 5) Very important.

The item questions and measurement variables that constitute the management support construct are presented in Table 7.7.

Table 7.7: Management support construct and measurement variables

Measurable construct	Measurable variable	Item variable
Management support	Policy approval	The involvement of executive management in the information security policy development is crucial to the approval of the security policies.
	Policy enforcement	Top management plays a significant role in enforcing the information security policy so as to ensure that employees regard the policy requirements in a serious light.
	Management involvement	Executive management is involved in the whole process of information security policy development.
	Budget	Executive management must ensure sufficient budget is available for the information security policy development.

The following section highlights the employee support construct.

7.2.7 Employee support construct

The questions asked in this category were intended to determine the level of importance of the employee support processes.

Question: Please indicate the importance of each of the following employee support processes 1) Not important, 2) Somewhat important, 3) Neutral, 4) Important and 5) Very important.

The item questions and measurement variables that constitute employee support construct are presented in Table 7.8.

Table 7.8: Employee support construct and measurement variables

Measurement construct	Measurement variable	Item variable
Employee support	Deterrence measure	There should be mechanisms in place to punish employees who intentionally violate the information security policy.
	Binding agreement	Employees should sign that they have received and reviewed the policies and agree to be bound by such policies.
	Job termination	Job termination should be considered for employees who repeatedly violate the information security policy.
	Employee involvement	The involvement of employees during the formulation of the information security policy requirements enhances compliance with such security policy requirements.

The next section discusses the information security policy compliance construct.

7.2.8 Information security policy compliance construct

The questions asked in this category were intended to determine the level of importance of the information security policy compliance processes.

Question: Please indicate the importance of each of the following information security policy compliance processes 1) Not important, 2) Somewhat important, 3) Neutral, 4) Important and 5) Very important.

The item questions and measurement variables that constitute information security policy compliance construct are shown in Table 7.9. These measurement and items variables are directly referred from Bulgurcu et al. (2010).

Table 7.9: Information security policy compliance construct and measurement variables

Measurement construct	Measurement variable	Item variable
Information security policy compliance	Attitude	"An employee's positive attitude towards compliance with the organisation's information security policy positively influences his/her intention to comply with the requirements of the information security policy."
	Perceived social pressure	"An employee's perceived social pressure about his/her compliance with the requirements of the information security policy positively influences his/her intention to comply with the requirements of the information security policy."
	Perceived benefit	"An employee's perceived benefit of compliance with the organisation's information security policy positively influences his/her attitude towards complying with the requirements of the information security policy."
	Knowledge	"An employee's judgment of his / her own knowledge in complying with the requirements of the information security policy positively influences his/her intention to comply with the requirements of the information security policy."

The next section discusses the validity and reliability of the questionnaire variables.

7.3 Validity and reliability of the questionnaire variables

Tavakol and Dennick (2011) maintain that reliability and validity are two fundamental elements in the assessment of a measurement instrument. In this research project Cronbach's alpha was used to measure the internal consistency of the questionnaire variables. "Internal consistency describes the extent to which all items in a test measure the same concept or construct and, hence, it is connected to the inter-relatedness of the items within the test" (Tavakol and Dennick, 2011). Raerd (2012) indicates that Cronbach's alpha is the most commonly used statistical test to determine the reliability of multiple Likert-type questions in a survey.

This chapter also investigates the reliability and validity of the seven constructs of the proposed framework.

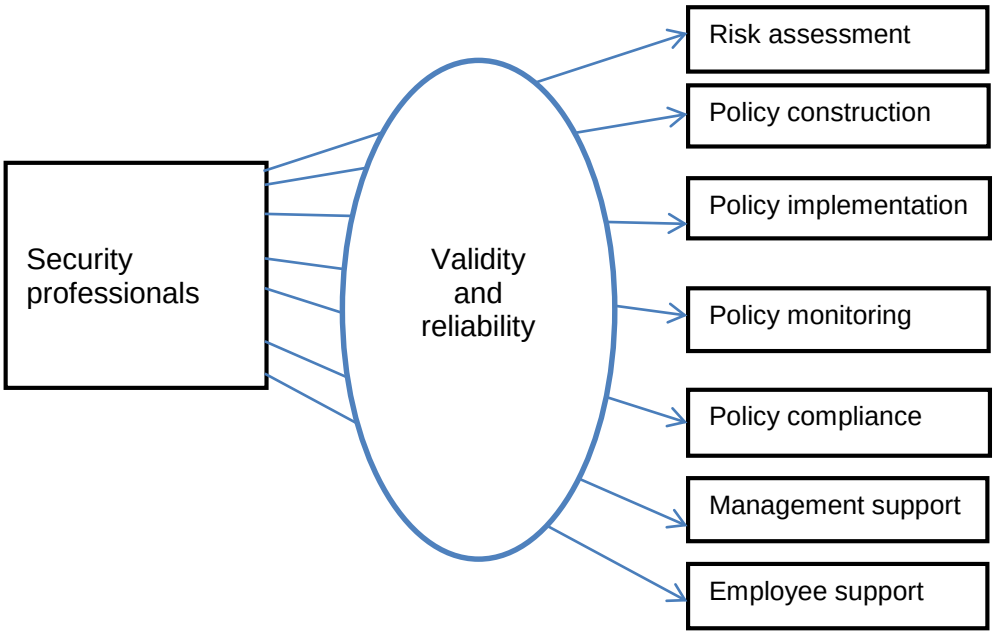


Figure 7.1: Reliability statistics for constructs

7.3.1 Reliability statistics of the combined constructs

Cronbach's alpha was used to measure the reliability of the questions relating to the importance of the seven constructs of the proposed framework. As depicted in Table 7.10, the Cronbach's alpha was α = 0. 943. This, in turn, shows that the sub-variables asked in the questionnaire in relation to all the combined constructs of the framework were both reliable and consistent. A Cronbach's alpha value of 0.7 or greater is considered acceptable (Gefen et al., 2000; Nunnally and Bernstein, 1994).

Table 7.10: Reliability Statistics for combined constructs

Cronbach's Alpha	Cronbach's Alpha based on standardised items	N of Items
. 943	. 943	7

The next section discusses the reliability statistical result of each of the seven constructs depicted in Figure 7.1.

7.3.2 Reliability statistics of the risk assessment construct

Cronbach's alpha was used to establish the internal consistency of the questions related to risk assessment. As shown in Table 7.11, the Cronbach's alpha was $\alpha = 0.916$. This, in

turn, shows that the sub-variables asked in the questionnaire in relation to risk assessment construct were both reliable and consistent.

Table 7.11: Reliability Statistics for the risk assessment

Cronbach's Alpha	Cronbach's Alpha based on standardised items	N of Items
. 916	. 916	4

The next section discusses the reliability statistics of information security policy construction construct.

7.3.3 Reliability statistics of the information security policy construction construct

Cronbach's alpha was used to establish the internal consistency of the questions related to risk assessment. As depicted in Table 7.12, the Cronbach's alpha value of α = 0. 907 indicates that the sub-variables asked in the questionnaire were both reliable and consistent as regards the information security policy construction construct.

Table 7.12: Reliability Statistics for information security policy construction

Cronbach's Alpha	Cronbach's Alpha based on standardised items	N of Items
. 907	. 908	4

The next section discusses the reliability statistics of information security policy implementation construct.

7.3.4 Reliability statistics of the information security policy implementation construct

Cronbach's alpha was used to establish the internal consistency of the scales of the questions relating to information security policy implementation. As shown in Table 7.13, the Cronbach's alpha value of α = 0. 894 indicates that the sub-variables asked in the questionnaire were both reliable and consistent as regards the information security policy implementation processes.

Table 7.13: Reliability Statistics for information security implementation

Cronbach's Alpha	Cronbach's Alpha based on standardised items	N of Items
. 894	. 895	4

The next section discusses the reliability statistics of information security policy monitoring and review construct.

7.3.5 Reliability statistics of the information security policy monitoring and review

Cronbach's alpha was used to establish the internal consistency of the questions related to information security policy assessment and monitoring. As depicted in Table 7.14, the Cronbach's alpha was α = 0. 898. This, in turn, indicates that the sub-variables asked in the questionnaire in relation to the information security policy assessment and monitoring processes were both reliable and consistent.

Table 7.14: Reliability Statistics for information security policy monitoring and review

Cronbach's Alpha	Cronbach's Alpha based on standardised items	N of Items
. 898	. 898	4

The next section discusses the reliability statistics of management support construct.

7.3.6 Reliability statistics of management support

Cronbach's alpha was used to establish the internal consistency of the scales of the questions relating to management support. As depicted in Table 7.15, the Cronbach's alpha was α = 0. 904, indicating that the sub-variables asked in the questionnaire in relation to management support were both reliable and consistent.

Table 7.15: Reliability Statistics for management support

Cronbach's Alpha	Cronbach's Alpha based on standardised items	N of Items
. 904	. 905	4

The next section discusses the reliability statistics of employee support construct.

7.3.7 Reliability statistics of the employee support construct

Cronbach's alpha was used to establish the internal consistency of the questions relating to employee support. As depicted in Table 7.16, the Cronbach's alpha was α = 0. 900, indicating that the sub-variables asked in the questionnaire in relation to employee support were both reliable and consistent.

Table 7.16: Reliability Statistics for employee support

Cronbach's Alpha	Cronbach's Alpha based on standardised items	N of Items
. 900	. 901	4

The following section highlights the reliability statistics of information security policy compliance construct.

7.3.8 Reliability statistics of information security policy compliance construct

Cronbach's alpha was used to determine the internal consistency of the scales of the questions relating to information security policy compliance. As shown in Table 7.17, the Cronbach's alpha was α = 0. 909, indicating that the sub-variables asked in the questionnaire in relation to information security policy compliance were both reliable and consistent.

Table 7.17: Reliability Statistics for information security policy compliance

Cronbach's Alpha	Cronbach's Alpha based on standardised items	N of Items
. 909	. 909	4

The following section highlights the reliability statistics of all questions.

7.3.9 Reliability statistics of all questions

Cronbach's alpha was used to establish the internal consistency of all the questions asked in the survey. As depicted in Table 7.18, the Cronbach's alpha was α = 0. 979, indicating that the sub-variables asked in the questionnaire regarding the composite of all the items asked in the questionnaire were both reliable and consistent.

Table 7.18: Reliability Statistics for the composite of all questions

Cronbach's Alpha	Cronbach's Alpha based on standardised items	N of Items
. 979	. 978	40

The next section concentrates on the descriptive statistical analysis and findings.

7.4 Descriptive statistical analysis and findings

This section discusses the statistical analysis and findings of the survey. Firstly, the findings of the demographic results are discussed and, secondly, the findings of each of the seven constructs of framework are discussed. This is followed by a discussion of the factors of each construct.

7.4.1 Demographic findings

This section discusses the findings relating to the demographic characteristics of the respondents.

7.4.1.1 Name of country

Respondents were asked to indicate in which country they lived – the United Kingdom or the United States of America. A total number of 329 security professionals (192 from UK and 137 from USA) responded to the survey. It emerged that 58.36% of the respondents lived in the United Kingdom while 41.64% lived in the United States of America. Figure 7.2 presents a diagrammatical representation of the percentages relating to the countries in which the respondents lived.

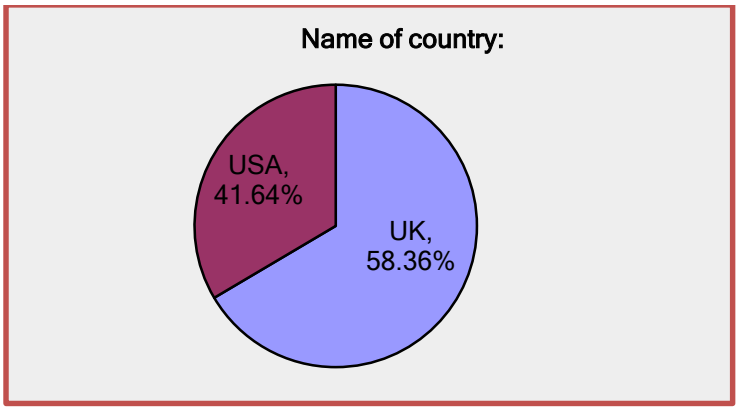


Figure 7.2: Respondents' country name

7.4.1.2 Organisation type

The respondents were asked to specify the type of organisation for which they worked. It emerged that 41.92% worked in industry; 17.69% in government; 14.23% in the banking sector; 13.46% in the consulting sector and 12.69% in the trading sector. Figure 7.3 presents the findings relating to the type of organisation for which the respondents worked.

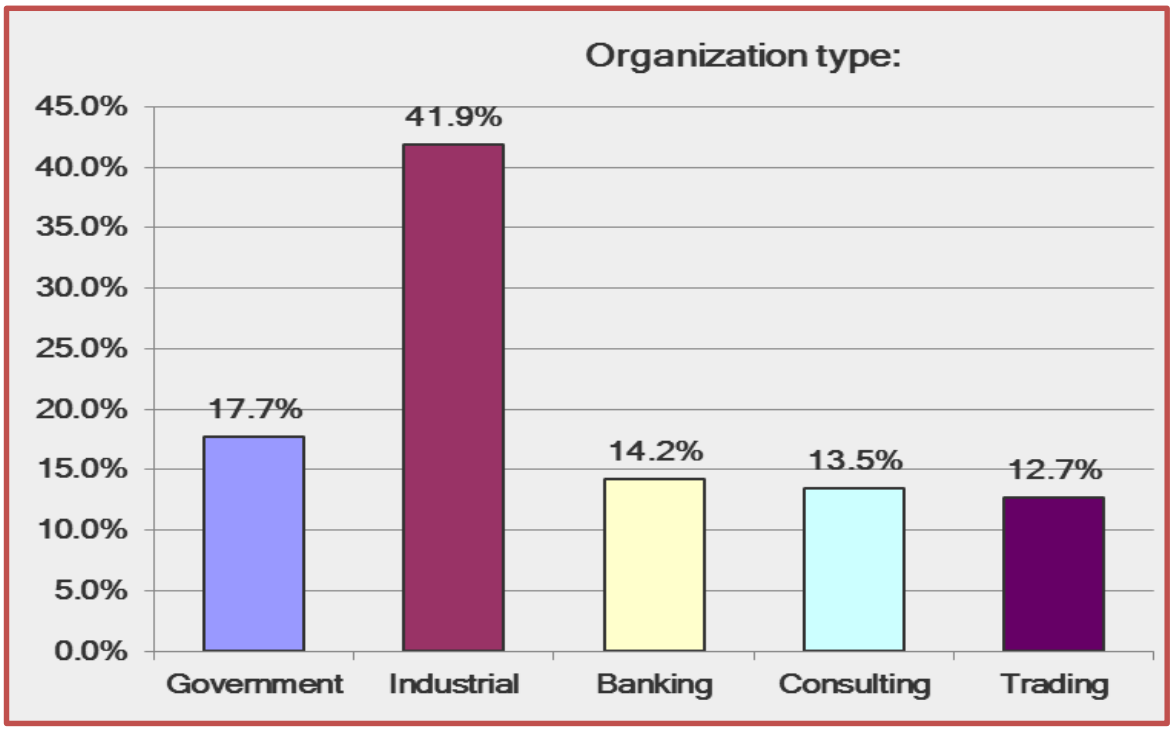


Figure 7.3: Respondents' organisation type

7.4.1.3 Respondents' occupations

The respondents were asked to specify their occupations. The results indicate a high percentage of IT managers (40.59%); 21.03% Chief Information Officers (CIO); 20.30% security specialists, and 18.08% IT consultants. Figure 7.4 presents the results of the respondents' occupations.

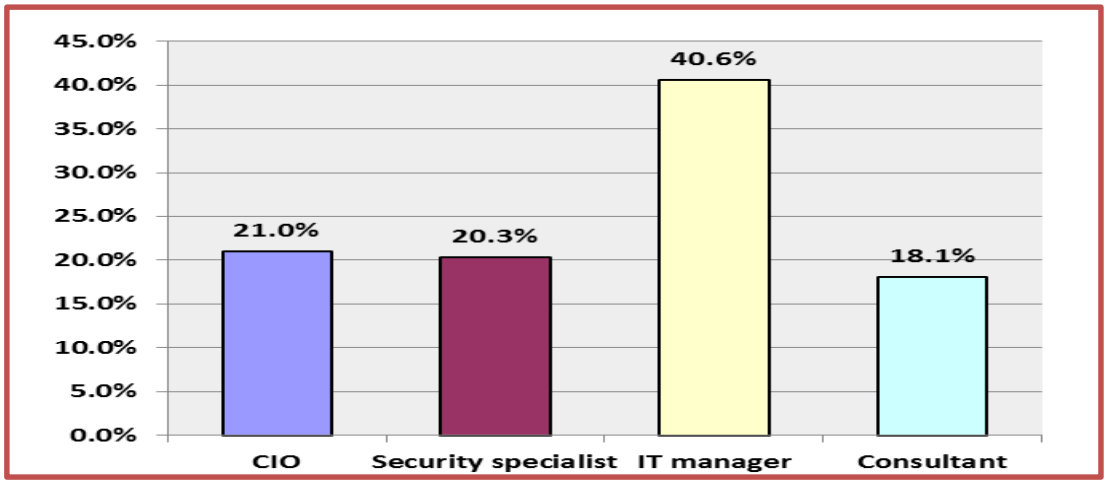


Figure 7.4: Respondents' occupations

7.4.1.4 Respondents' organisation size

The respondents were asked to indicate the number of employees working in their organisation. The findings revealed that 35.71% worked for organisation with less than 500 employees; 25.65% for organisations with between 500 and 1 000 employees; 23.70% for organisations with between 1 000 and 5 000 employees; 6.17% for organisations with between 5 000 and 10 000 employees, and 8.77% for organisations with more than 10 000 employees. Figure 7.5 presents the results pertaining to organisation size in terms of number of employees.

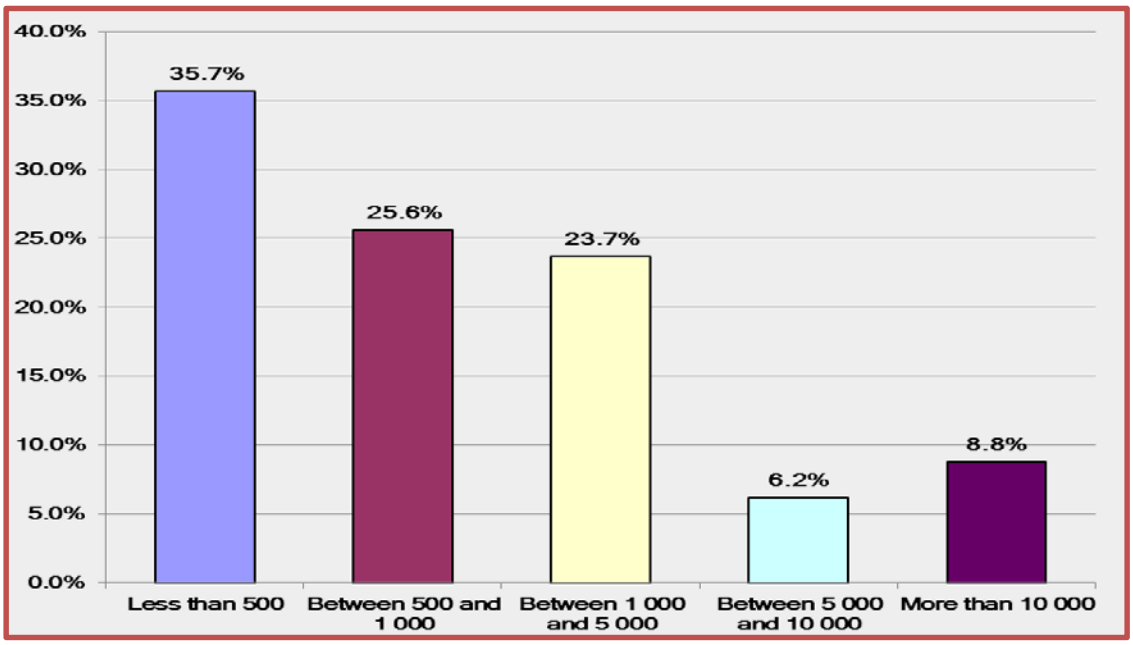


Figure 7.5: Organisation size

7.4.1.5 Organisations' information security policy

The respondents were asked to indicate whether an information security policy had been implemented in the organisations for which they worked. The majority of the respondents (85.53%) indicated that their organisations had implemented an information security policy while 14.47% stated that their organisations did not have such a policy in place. Figure 7.6 presents the findings.

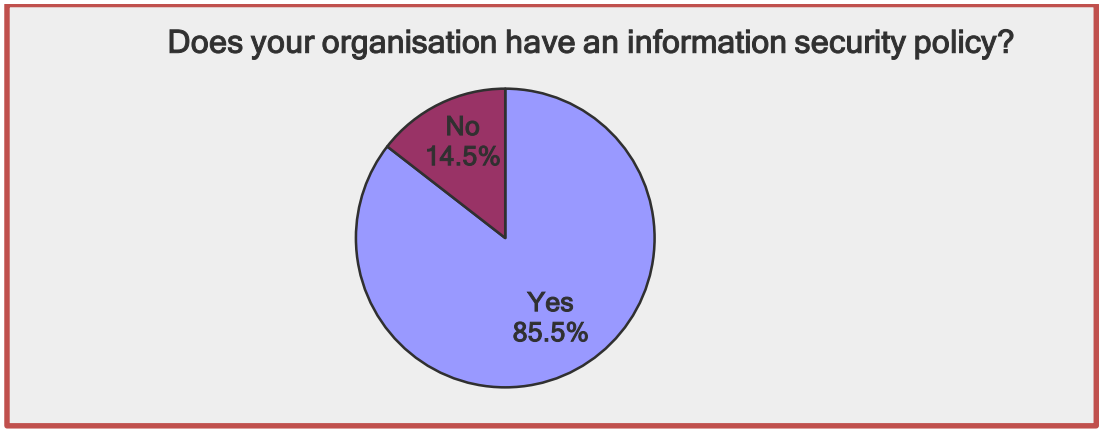


Figure 7.6: Organisations' information security policies

The next section discusses the findings of each construct.

7.4.2 Findings for each construct

Question: How important do you believe the following variables are for the successful implementation of an information security policy in your organisation? 1) Not important, 2) Somewhat important, 3) Neutral, 4) Important and 5) Very important.

7.4.2.1 Results of the risk assessment construct

The respondents were asked to indicate the importance of the following statement which is linked to risk assessment strategy: *Organisations should have a clear understanding of their organisation's security risks*. Figure 7.7 presents the findings diagrammatically.

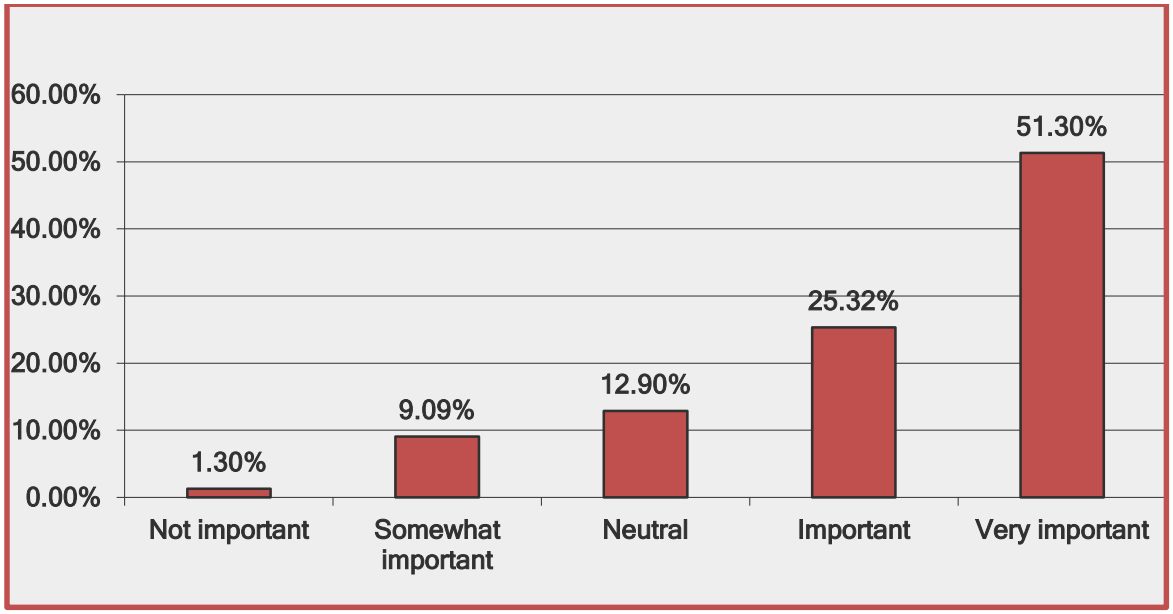


Figure 7.7: Results of the risk assessment construct

As shown in Figure 7.7, the majority of the respondents agreed on the importance of risk assessment processes with a total percentage of 51.30% stating that such processes are very important; 25.32% that they are important; 12.99% were neutral; 9.09% stating that they are somewhat important 1.30% stating that they are not important.

7.4.2.2 Results of the risk assessment sub-variables

A five-point Likert-type scale was used to ascertain the importance of the risk assessment sub-variable items. Table 7.19 presents a summary of the participants' responses with regards to the importance of the risk assessment processes.

Table 7.19: Results of the risk assessment sub-variables

	Assets identification	Vulnerabilities and threats	Risk identification	Legislation
Not important	1.6 %	1.3 %	1.6 %	1.3 %
Somewhat important	5.5 %	6.8 %	5.5 %	4.9 %
Neutral	16.5 % %	13.9 %	17.9 %	18.8 %
Important	36.5 %	32.7 %	36.7 %	35.4 %
Very important	40.0 %	45.3 %	38.3 %	39.6 %

Table 7.20 presents the descriptive statistics pertaining to the risk assessment sub-variables with the Mean values arranged from highest to lowest.

Table 7.20: Descriptive statistics results of risk assessment sub-variables

	N	Mean	Median	Std. Deviation
Vulnerabilities and threats	309	4.1392	3.0000	.98201
Assets identification	310	4.0774	3.0000	.96230
Legislation	308	4.0714	3.0000	.94547
Risk identification	308	4.0455	3.0000	.96412

As shown in Table 7.20, the results revealed that the mean was above 3 the middle value in the 5-point scale (Dewberry, 2004, p. 14). This, in turn, shows that the respondents deemed all four factors to be important. The identification of vulnerabilities and threats process had the highest mean of 4.1392. This, in turn, indicates that the respondents believed that this process is very important as compared to the other process of risk assessment construct.

As presented in Table 7.19, a total percentage of 45.3% of the respondents indicated that developing a risk assessment plan that includes the assessment of vulnerabilities and security threats is very important; 32.7% stated that it was important; 13.9% were neutral; 6.8% deemed it somewhat important while 1.3% stated that it was not important. The results show that the respondents believed that the identification of risks was the least important (Mean = 4.0455) of all the risk assessment factors.

7.4.2.3 Results of the information security policy construction construct

The respondents were asked to indicate the importance of the following statement which is linked to the information security policy construction process: *The information security policy construction process should be based on the findings and recommendations of the of risk assessment processes*. Figure 7.8 presents the results diagrammatically.

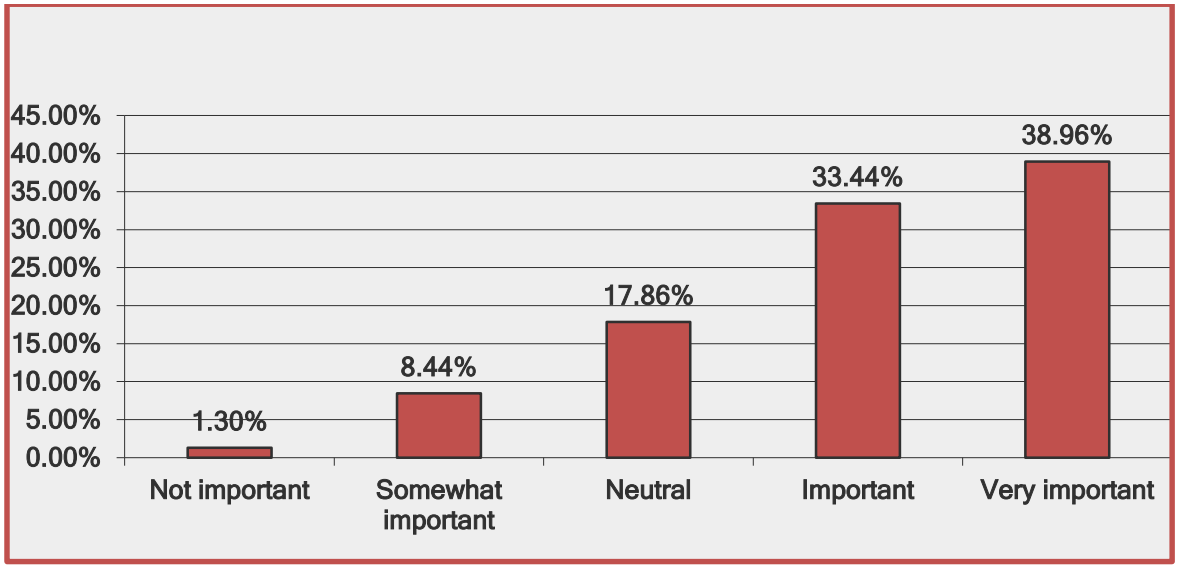


Figure 7.8: Findings pertaining to the information security policy construction construct

As shown in Figure 7.8, the majority of the respondents agreed on the importance of the information security policy construction process with a total percentage of 38.96% the respondents stating that it is very important; 33.44% stating that it is important; 17.86% were neutral; 8.44% stating that it is somewhat important and 1.30% stating that it is not important.

7.4.2.4 Results of the information security policy construction sub-variables

A five-point Likert-type scale was used to ascertain the importance of the information security policy construction sub-variable items. Table 7.21 presents the results.

Table 7.21: Results of the information security policy construction sub-variables

	Consultation with stakeholders	Write high level security policy	Write detailed security policy	Write lower level security policy
Not important	2.6 %	1.3 %	1.3 %	2.9 %
Somewhat important	8.8 %	7.1 %	5.2 %	6.8 %
Neutral	19.2 %	20.4 %	19.5 %	24.2 %
Important	39.1 %	36.6 %	44.0 %	40.0 %
Very important	30.3 %	34.6 %	30.0 %	26.1 %

Table 7.22 presents the descriptive statistics pertaining to the information security policy construction sub-variables with the Mean values arranged from highest to lowest.

Table 7.22: Results of the information security policy construction sub-variables

	N	Mean	Median	Std. Deviation
Write detailed security policy	306	3.9804	3.0000	.93015
Write high level security policy	309	3.9612	3.0000	.97623
Consultation with stakeholders	307	3.9609	3.0000	.90664
Write lower level security policy	307	3.8567	3.0000	1.03168

As shown in Table 7.22, the results revealed that the mean was above 3 the middle value in the 5-point scale (Dewberry, 2004, p. 14). This, in turn, shows that respondents deemed all four factors to be important. The development of detailed security policies had the highest mean of 3.9804, indicating that the respondents believed that this process was very important as compared to the other process of the information security policy construction construct.

As highlighted in Table 7.21, the results show that 30.0% of the respondents stated that developing detailed security policies (detailed statements of strategic level policies showing what should be done in order to comply with the security policy) was very important; 44.0% stated that it was important; 19.5% were neutral; 5.2% stated that it is somewhat important, while 1.3% stated that it was not important. The respondents indicated that the construction of the lower level security policies was the least important (Mean = 3.8567) of the factors relating to information security policy construction. The next section discusses the results of the information security policy implementation.

7.4.3 Results of the information security policy implementation construct

The respondents were asked to indicate the importance of the following statement which is linked to information security policy implementation process: S*uitable information security policy training and education are essential during the information security policy implementation stage*. Figure 7.9 presents the findings diagrammatically.

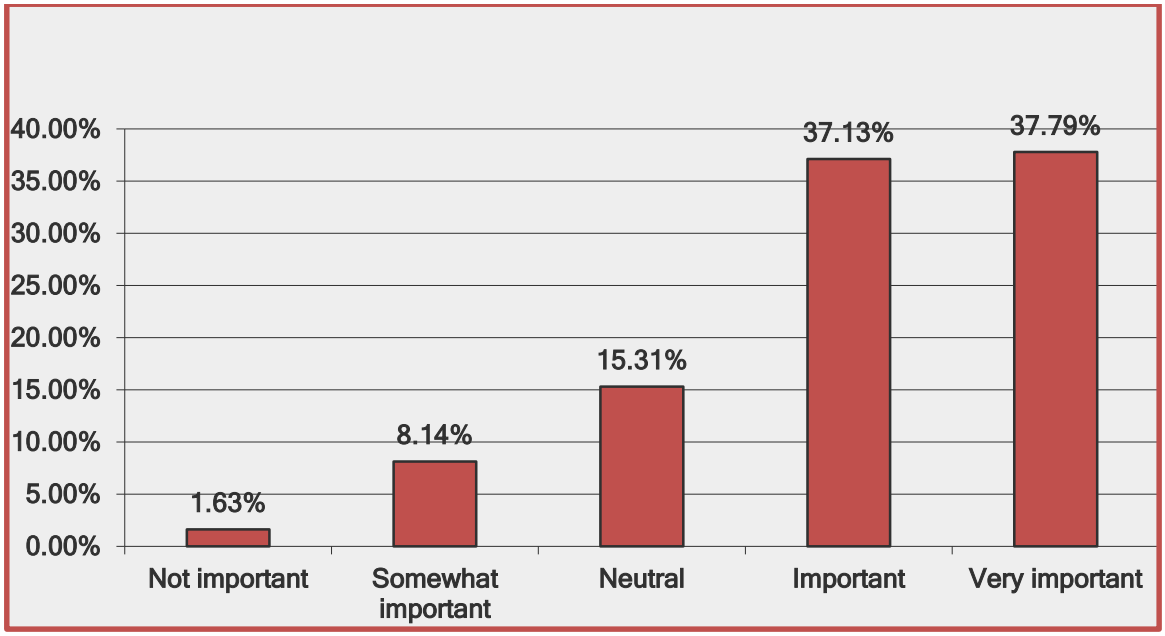


Figure 7.9: Findings of the information security policy implementation construct

As shown in Figure 7.9, the majority of respondents agreed on the importance of the information security policy implementation process with 37.79% stating that was very important; 37.13% that it was important; 15.31% were neutral; 8.14% that it was somewhat important, while 1.63% stated that it was not important.

7.4.3.1 Findings of the information security policy implementation sub-variables

A five-point Likert-type scale was used to ascertain the importance of the information security policy implementation sub-variable items. Table 7.23 presents the results.

Table 7.23: Findings of information security policy implementation sub-variables

	Security policy awareness	Security policy training	Stakeholders' role	Security policy education
Not important	2.9 %	1.3 %	1.6 %	1.3 %
Somewhat important	6.8 %	6.8 %	5.5 %	7.1 %
Neutral	24.2 %	20.7 %	18.4 %	18.1 %
Important	40.0 %	39.2 %	34.6 %	33.7 %
Very important	26.1 %	32.0 %	39.8 %	39.8 %

Table 7.24 presents the descriptive statistics pertaining to the information security policy implementation sub-variables with the mean values arranged from highest to lowest.

Table 7.24: Findings of information security policy implementation sub-variables

	N	Mean	Median	Std. Deviation
Role of stakeholders	309	4.0550	3.0000	.97379
Security policy education	309	4.0356	3.0000	.99121
Security policy training	309	3.9385	3.0000	.95658
Security policy awareness	310	3.7968	3.0000	.99870

As shown in Table 7.24, the results revealed that the mean was above 3 the middle value in the five-point scale (Dewberry, 2004, p. 14). This shows that respondents deemed all four factors to be important. Defining the role of stakeholders had the highest mean of 4.0550, indicating that he respondents believed that this process was very important as compared to the other process of the information security policy implementation construct.

As highlighted in Table 7.23, it was found a 39.8% of the respondents stated that defining the roles of the various organisation stakeholders (executive management, information security officials, all employees) was very important; 34.6% stated that it was important; 18.4% were neutral; 5.5% stated that it was somewhat important, while 1.6% stated that it was not important.

7.4.4 Findings of the information security policy monitoring and review construct

The respondents were asked to indicate the importance of the following statement which is linked to the information security policy monitoring and review process: *Regularly assess and monitor the information security policies to ensure that they are effective*. Figure 7.10 presents the findings.

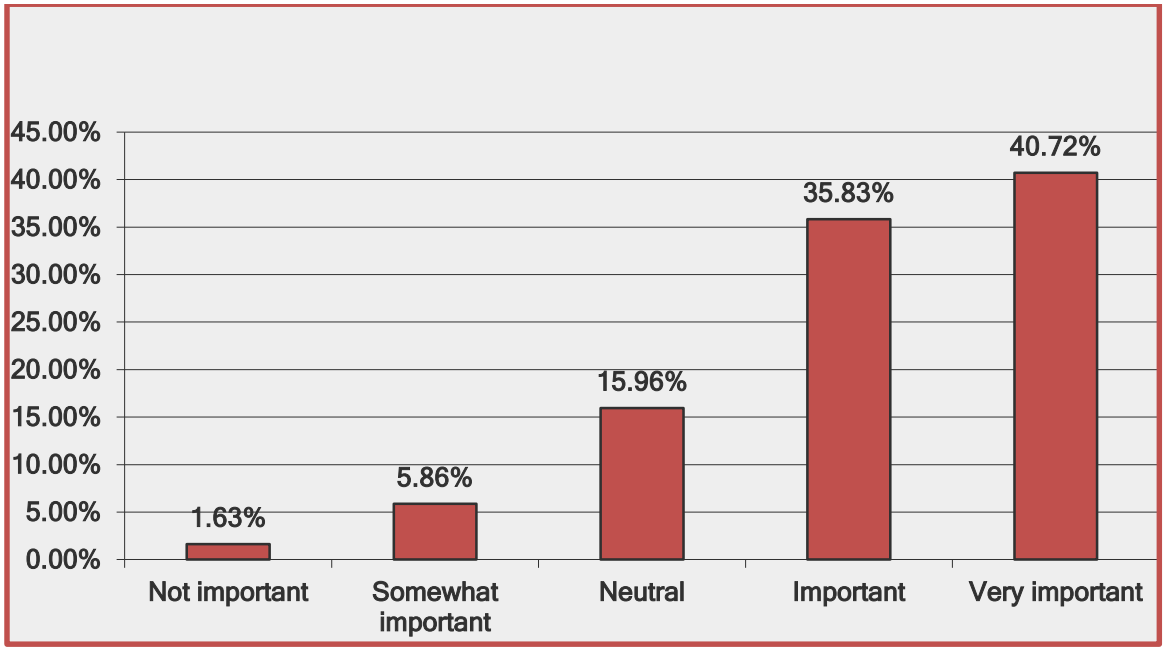


Figure 7.10: Findings of information security policy monitoring and review

As shown in Figure 7.10, the majority of the respondents agreed on the importance of the information security policy monitoring and review process with a 40.72% of the respondents agreeing that it was very important; 35.83% that it was important; 15.96% were neutral; 5.86% agreed it was somewhat important, while 1.63% stated that it was not important. Information security policy monitoring and review helps to identify the users' activities as regards information security policy compliance.

7.4.4.1 Findings of the information security policy monitoring and review sub-variables

A five-point Likert-type scale was used to ascertain the importance of the information security policy monitoring and assessment sub-variable items. Table 7.25 presents the results.

Table 7.25: Findings of information security policy monitoring and sub-variables

	Periodic review	Automated review	Audit of information	Non periodic review
Not important	1.0 %	2.0 %	1.9 %	2.3 %
Somewhat important	7.8 %	6.9 %	4.8 %	4.2 %
Neutral	17.2 %	20.3 %	19.0 %	19.9 %
Important	36.7 %	40.5 %	38.1 %	39.1 %
Very important	37.3 %	30.4 %	36.1 %	34.5 %

Table 7.26 presents the descriptive statistics pertaining to the information security policy monitoring and assessment sub-variables with the mean values arranged from the highest to the lowest.

Table 7.26: Descriptive statistics results of information security policy monitoring sub-variables

	N	Mean	Median	Std. Deviation
Periodical review	308	4.0162	3.0000	.97346
Audit information	310	4.0161	3.0000	.96024
Non periodical review	307	3.9935	3.0000	.95996
Automated review	306	3.9052	3.0000	.97552

As shown in Table 7.26, the results revealed that the mean was above 3 the middle value in the five-point scale (Dewberry, 2004, p. 14). This, in turn, shows that respondents deemed all four factors to be important. The periodical review during information security policy monitoring and assessment sub-variable had the highest mean of 4.0162, indicating that the respondents believed that this process was very important as compared to the other processes of the information security policy monitoring and assessment construct.

As highlighted in Table 7.25, it emerged that 37.3% of the respondents believed that reviewing the information security policy on a regular basis to ensure that the latest threats and new regulations are kept up-to-date was very important; 36.7**%** stated that it was important; 17.2% were neutral; 7.8% stated it was somewhat important, while 1.0% stated that it was not important. The respondents indicated that the automated review was the least important (mean = 3.9052) of all the factors of the information security policy monitoring and assessment construct. The next section discusses the results of the information security policy compliance.

7.4.5 Findings of information security policy compliance construct

The respondents were asked to indicate the importance of the following statement which is linked to the information security policy compliance process: *There should be effective information security policy compliance mechanisms to ensure that employees adhere to an organisation's information security policy requirements.* Figure 7.11 presents the findings.

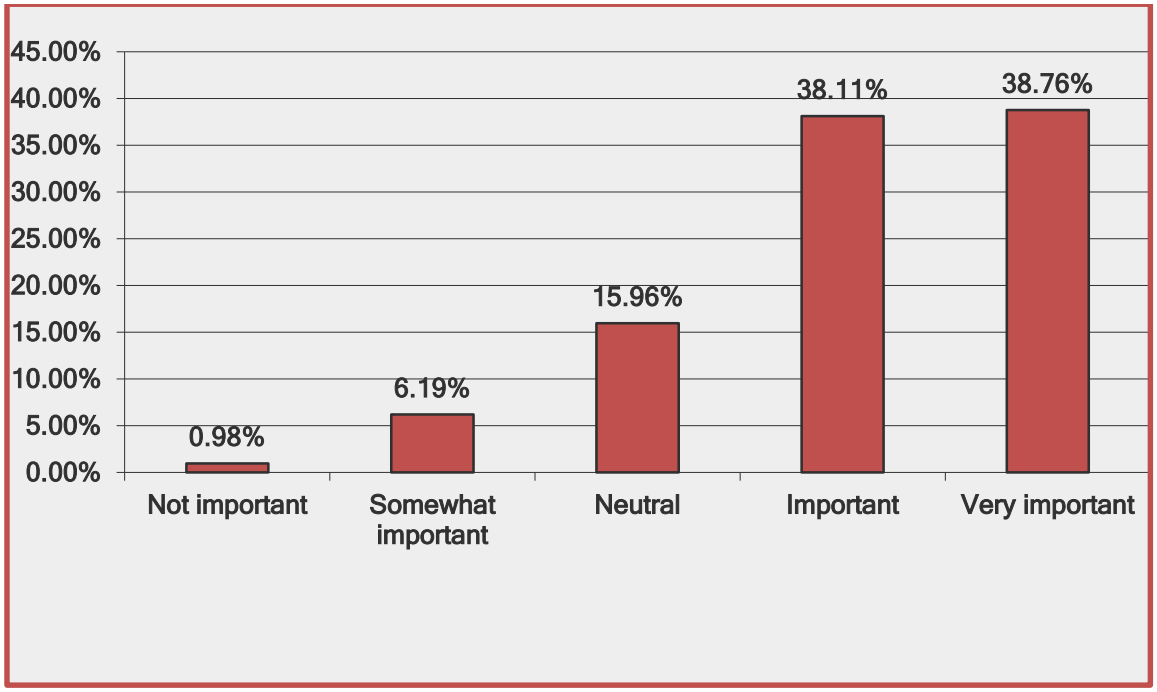


Figure 7.11: Findings of the information security policy compliance

As shown in figure 7.11, the majority of respondents agreed on the importance of the information security policy compliance process with 38.76% stating that it was very important; 38.11% that it was important; 15.96% were neutral; 6.19% stating that it was somewhat important, while 0.98% stated that it was not important.

7.4.5.1 Findings of information security policy compliance sub-variables

A five-point Likert-type scale was used to ascertain the importance of the information security policy compliance sub-variable items. Table 7.27 presents the results.

Table 7.27: Findings of the information security policy compliance sub-variables

	Attitude	Perceived social pressure	Perceived benefit	Knowledge
Not important	1.3 %	1.6 %	1.0 %	0.7 %
Somewhat important	4.5 %	4.6 %	4.2 %	5.9 %
Neutral	19.5 %	23.1 %	23.8 %	19.7 %
Important	43.8 %	36.2 %	38.1 %	41.0 %
Very important	30.8 %	34.5 %	32.9 %	32.8 %

Table 7.28 presents the descriptive statistics pertaining to the information security policy compliance sub-variables with the mean values ordered from the highest to the lowest.

Table 7.28: Findings of the information security policy compliance sub-variables

	N	Mean	Median	Std. Deviation
Knowledge	305	3.9934	3.0000	.90682
Attitude	308	3.9838	3.0000	.89683
Perceived benefit	307	3.9772	3.0000	.90900
Perceived social pressure	307	3.9739	3.0000	.95279

As highlighted in Table 7.28, the results revealed that the mean was above 3 the middle value in the five-point scale (Dewberry, 2004, p. 14). This, in turn, shows that the respondents deemed all these factors to be important. Knowledge emerged as an important factor of information security policy compliance with the highest mean of 3.9934, thus indicating that the respondents believed that this process is very important as compared to the other processes of the information security policy compliance construct.

As shown in Table 7.27, it was found that 32.8% of the respondents agreed that an employee's positive attitude towards compliance with the organisation's information security policy positively influences his/her intention to comply with the requirements of the information security policy; 41.0**%** stated that this was important; 19.7% were neutral; 5.9% stated it was somewhat important, while 0.7% stated that it was not important. The respondents indicated that perceived social pressure was the least important (Mean = 3. 9739) of the factors of the information security policy compliance construct. The next section discusses the findings of management support construct.

7.4.6 Results of the management support construct

The respondents were asked to indicate the importance of the following statement which is linked to top management support: *Organisations should have visible support and commitment from the top executive management.* Figure 7.12 presents the findings.

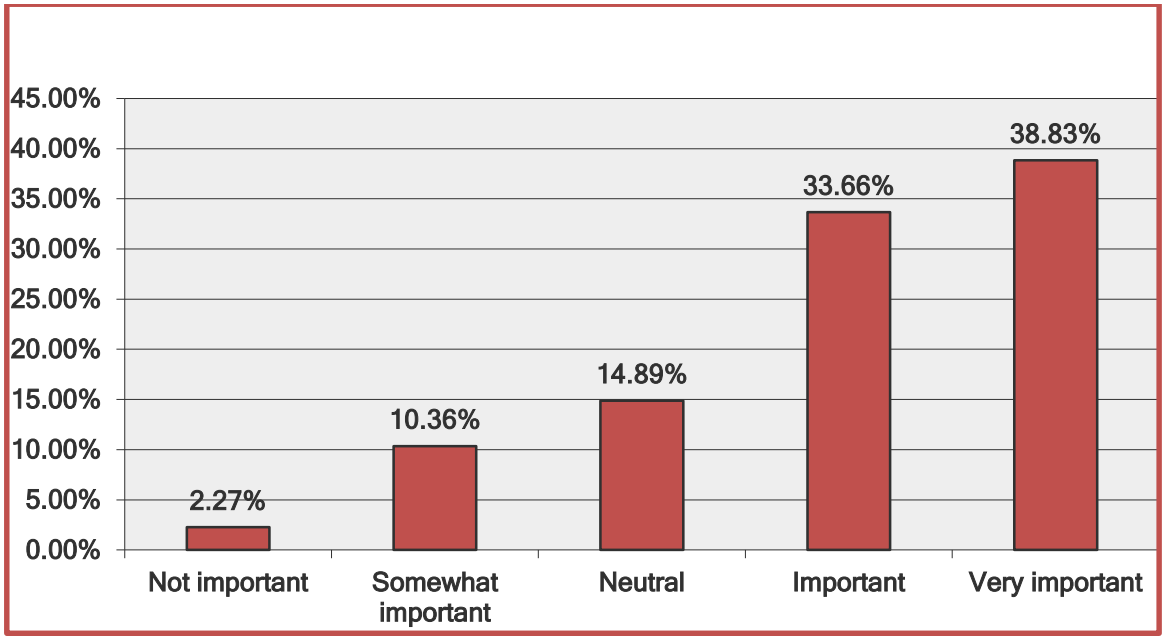


Figure 7.12: Results of the management support construct

As shown in Figure 7.12, the majority of the respondents agreed on the importance of management support with 38.83% stating that it was very important; 33.66% that it was important; 14.89% were neutral; 10.36% stating that it was somewhat important, while 2.27% stated that it was not important.

7.4.6.1 Findings of management support sub-variables

A five-point Likert-type scale was used to ascertain the importance of the management support sub-variable items. Table 7.29 presents the results.

Table 7.29: Results of management support sub-variables

	Management involvement	**Budget**	**Policy enforcement**	**Policy approval**
Not important	1.0 %	1.6	1.9	1.6
Somewhat important	5.8 %	5.2	6.5	6.2
Neutral	18.5 %	17.6	18.5	20.7
Important	37.0 %	38.8	33.8	38.4
Very important	37.7 %	36.8	39.3	33.1

Table 7.30 presents the descriptive statistics of the management support sub-variables with the mean values arranged from the highest to the lowest.

Table 7.30: Results of management support sub-variables

	N	Mean	Median	Std. Deviation
Management involvement	308	4.0455	3.0000	.94017
Budget	307	4.0391	3.0000	.94891
Policy enforcement	308	4.0195	3.0000	1.00792
Policy approval	305	3.9508	3.0000	.96699

As shown in Table 7.30, the results revealed that the mean was above 3 the middle value in the five-point scale (Dewberry, 2004, p. 14). This, in turn, shows that the respondents deemed all these factors to be important. Management involvement had the highest mean of 4.0455, indicating that the respondents believed that this process is very important as compared to the other process of the management support construct.

As highlighted in Table 7.29, it was found that 37.7% of the respondents agreed that the involvement of executive management in the whole process of information security policy was very important; 37.0**%** stated that it was important; 18.5% were neutral; 5.8% stated that it was somewhat important, while 1.0% stated that it was not important.

7.4.7 Results of the employee support construct

The respondents were asked to indicate the importance of the following statement which is linked to employee support: *Ensure that employees support and understand their roles and responsibilities in respect of the information security policy requirements.* Figure 7.13 presents the findings.

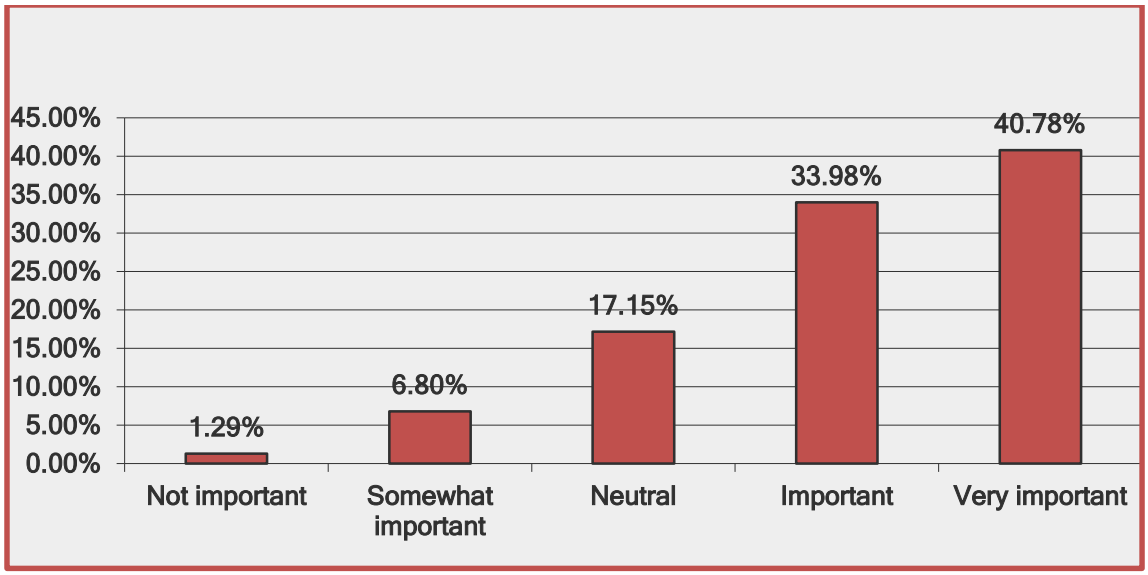


Figure 7.13: Results of the employee support construct

As shown in Figure 7.13, the majority of the respondents agreed on the importance of employee support with 40.78% stating that it was very important; 33.89% that it was important; 17.15% were neutral; 6.80% stated that it was somewhat important while 1.29% stated that it was not important.

7.4.7.1 Results of the employee support sub-variables

A five-point Likert-type scale was used to ascertain the importance of the employee support sub-variable items. Table 7.31 presents the findings.

Table 7.31: Results of employee support sub-variables

	Deterrence measure	**Binding agreement**	**Employee involvement**	**Job termination**
Not important	2.3 %	2.3 %	1.6 %	1.0 %
Somewhat important	7.5 %	6.5 %	6.8 %	5.2 %
Neutral	22.5 %	17.2 %	20.2 %	19.5 %
Important	39.1 %	37.5 %	33.9 %	38.1 %
Very important	28.7 %	36.6 %	37.5 %	36.2 %

Table 7.32 presents the descriptive statistics of the employee support sub-variables with the mean values arranged from the highest to the lowest.

Table 7.32: Results of the employee support sub-variables

	N	Mean	Median	Std. Deviation
Employee involvement	307	4.0326	3.0000	.92474
Binding agreement	309	3.9968	3.0000	1.00162
Job termination	307	3.9870	3.0000	.99991
Deterrence measure	307	3.8436	3.0000	.99754

As highlighted in Table 7.32, the results revealed that the mean was above 3 the middle value in the five-point scale (Dewberry, 2004, p. 14). This, in turn, shows that the respondents deemed all four factors to be important. Employee involvement had the highest mean of 4.0326, thus indicating that the respondents believed that this process was very important as compared to the other processes of the employee support construct.

As presented in Table 7.31, it was found that 37.5% of the respondents agreed that the involvement of employees during the formulation of the information security policy requirements enhanced the compliance with such information security policy was very

important; 33.9% stated that it was important; 20.2% were neutral; 6.8% stated it was somewhat important, while 1.6% stated that it was not important. The respondents believed that the deterrence measures which highlight that there should be mechanisms in place to punish employees who intentionally violate the information security policy was the least important (Mean = 3.8436) of the factors of the employee support construct.

7.4.8 Overall findings

Table 7.33 presents the descriptive statistics of the seven constructs with the mean values arranged from the highest to the lowest.

Table 7.33: Descriptive statistics of the overall results

	N	Mean	Median	Std. Deviation
Risk assessment	308	4.1623	3.0000	1.04909
Management support	309	4.0814	3.0000	.97177
Information security policy compliance	307	4.0749	3.0000	.93808
Employee support	309	4.0615	3.0000	.98335
Information security policy implementation	307	4.0130	3.0000	1.00318
Information security policy construction	308	4.0032	3.0000	1.01294
Information policy monitoring and review	307	3.9644	3.0000	1.07602

As highlighted in Table 7.33, the results revealed that the mean of all seven constructs was above 3 the middle value in the five-point scale (Dewberry, 2004, p. 14). This, in turn, shows that the respondents deemed all seven factors to be important. Risk assessment had the highest mean of 4.1623, thus indicating that the respondents believed that this process was very important as compared to other the processes of the information security development life cycle. In addition, the respondents felt that management support, information security policy compliance and employee support were crucial.

7.4.8.1 Discussion of the overall findings

Descriptive statistics were used to measure the level of importance of the framework constructs. The mean of all seven of the constructs was above 3 the middle value in the five-point scale (Dewberry, 2004, p. 14). Thus, the results of the descriptive statistics revealed that, in general, the respondents agreed that all seven constructs of the proposed framework were important.

As shown in Table 7.33, the overall results showed that risk assessment was the most important construct of the seven constructs measured. This result is not surprising because the main reason for developing information security policies is to mitigate the various security risks that organisations face and, thus, risk assessment is a crucial step in the process. As one expert mentioned during the expert review of the framework (Chapter 8): "One of the drivers of security policy development is risk management, which is the whole reason for the existence of security policies."

The second most important construct was management support. Management plays a significant role in decision making in organisations. As stated by Kadam (2007), the involvement of executive management in the information security policy development is a key success factor in the development and implementation of security policies. The respondents also believed that information security policy compliance and employee support are important steps during an information security development and implementation development process. The overall results showed that information security policy monitoring was the least important of the seven constructs, thus indicating that this area requires more attention. Therefore, one of the objectives of this study is to integrate maturity assessment is the information security policy development life cycle. The following section discusses the findings of the open ended questions.

7.5 Analysis of the findings of the qualitative data collected from the open ended questions

The survey contained open ended questions in which respondents were asked to include any process that they deemed to be important for any of the constructs referred to in the questionnaire. Creswell (2009) maintains that one of the main advantages of open ended questions is that they enable participants to express their views in an unconstrained manner. The analysis of the open ended questions was based on the thematic analysis approach. Braun and Clarke (2006) define thematic analysis as a "qualitative analytic method for identifying, analysing and reporting patterns (themes) within data." Based on the respondents' comments, various themes related to the objectives of this research project were identified. The words and phrases that were related to the framework constructs were extracted from the responses of the respondents. The results of the open ended questions are presented in Table 7.34.

Table 7.34: Content analysis of open ended questions

	Factors identified	Risk assessment	Policy construction	Policy implementation	Policy monitoring	Policy compliance	Management support	Employee support	Stakeholders support
"Once a risk has been identified, there is a need to **evaluate existing security measures** to see if they can mitigate the risk or whether new security measures are needed to counter the threats."	Evaluating existing security measures	X							
"Security policy team needs to involve other stakeholders who will be affected by the new security policy. These include, for example, clients."	Clients stakeholders								X
"It is important that organisations specify their **risk appetite** or what risks they are willing to accept?"	Risk appetite	X							
"**Security specialists** must be involved in the security policy development because of their expertise that might be lacking in the security policy team."	Security specialists								X
"Organisations will need to **document the risk assessment** information so that they can refer to these information should another similar risk happen in future."	Risk assessment documentation	X							
"An organisation's policy should be submitted to **HR department** so that the new policies are communicated to the whole organisation."	HR department								X
"It is important that the **legal team** is involved in the information security policy development to ensure that the organisations' policies are in line with government laws."	Legal stakeholders								X

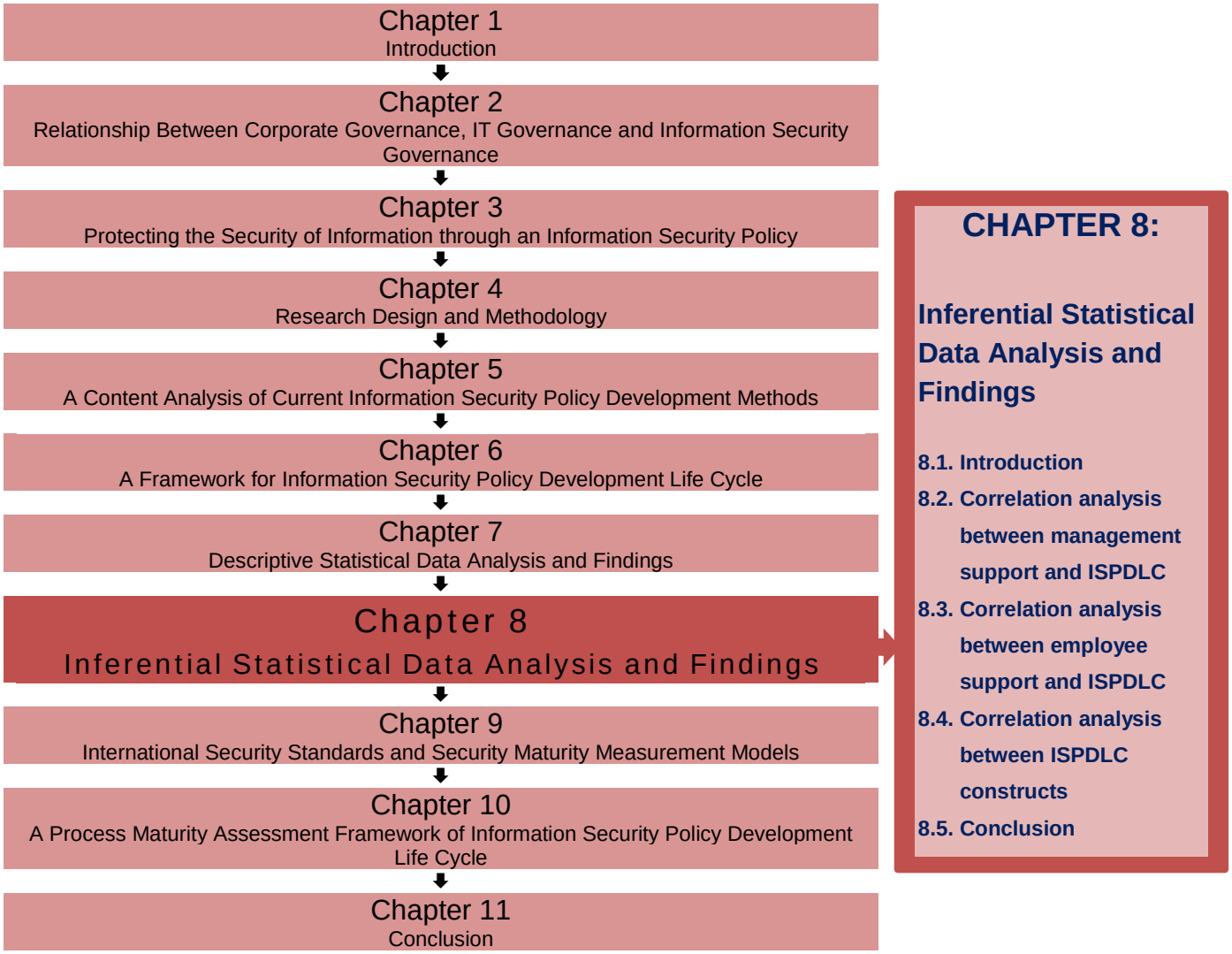
The factors that were identified in the content analysis presented in Table 7.34 were incorporated in the framework proposed in Chapter 7.

7.6 Conclusion

This chapter presents the findings of the data which was collected via the survey. Cronbach's alpha was used to measure the internal consistency of the questionnaire variables. Cronbach's alpha was $\alpha = 0.979$ for all 40 questions posed in the survey. This result confirms that the sub-variables asked in the questionnaire in relation to all the combined questions in the survey were both reliable and consistent.

This chapter also contained the findings of the qualitative data which was collected from open ended questions. The feedback comments of the respondents were analysed and new factors not included in the survey were identified. These factors were incorporated in the framework proposed in the chapter. The chapter also discussed the descriptive statistics that were used to assess the importance of the proposed framework constructs and its factors. Chapter 8 will discuss the inferential statistics that were used to explore the relationship between the constructs of the proposed framework.

Chapter 8: Inferential Statistical Data Analysis and Findings



8.1 Introduction

Chapter 7 discussed the descriptive statistical data analysis and findings. However, this chapter focuses on the inferential statistical data analysis and findings. Crossman (2003) maintains that "inferential statistics is concerned with making predictions or inferences about a population from observations and analyses of a sample." According to Blaikie (2010), there are two main objectives of inferential analysis:

- to make estimates of population characteristics (parameters) from sample characteristics (statistics);
- and to establish whether differences or relationships within the sample may be expected, other than by chance and, thus, in the population from which the sample was drawn.

While descriptive statistics are used for the description of data such as the mean, mode and frequency distribution, the main objective of inferential statistics is to generalise the findings to a larger population from the sample group under study (Crossman, 2003). In this study, the findings from the sample group of 400 security professionals will be generalised to the entire population. The study used inferential statistics tests to investigate the relationship between management support, employee support and information security policy development life cycle constructs. These constructs are presented in Figure 8.1. The objectives of the inferential statistical data analysis are presented in Table 8.1.

The following abbreviations will be used when referring to the constructs of the proposed framework:

- ISPDLC: Information Security Development Life Cycle
- RA: Risk Assessment
- ISPC: Information Security Policy Construction
- ISPI: Information Security Policy Implementation
- ISPM: Information Security Policy Monitoring and assessment
- ISPCO: Information Security Policy Compliance
- MS: Management Support
- ES: Employee Support

Table 8.1 highlights the measurement construct, objective of measurement and the questionnaire reference.

Table 8.1: Objectives of the inferential statistical data analysis

Objective	Measurement construct	Objective of measurement	Questionnaire reference
Investigate the relationship between management support and the ISPDLC	MS and RA, ISPC, ISPI, ISPM, ISPCO	Measure the strength of the relationship between management support and ISPDLC constructs	Q.6 – Q.12
Investigate the relationship between employee support and the ISPDLC	ES and RA, ISPC, ISPI, ISPM, ISPCO	Measure the strength of the relationship between ISPDLC constructs	Q.6 – Q.12

The next section discusses the correlation analysis between management support and the ISPDLC constructs.

8.2 Correlation analysis between management support and the Information Security Policy Development Life Cycle (ISPDLC)

Objective: Investigate the relationship between management support and the ISPDLC constructs

In the proposed framework it was argued that it is essential that management support be involved in all the processes of the ISPDLC. This chapter discusses the statistical tests that were conducted to determine the relationship between the management support construct and the ISPDLC constructs. Correlation analysis was used to explore the extent (if any) to which management support may influence the ISPDLC processes. The correlation coefficients provide an indication of whether the relationship is a positive relationship (changes to constructs increase or decrease in the same direction) or a negative relationship (constructs respond in opposite directions).

8.2.1 Management support and risk assessment correlation analysis

As depicted in Table 8.2, Pearson's correlation coefficient was used to investigate the relationship between management support and the risk assessment constructs.

Table 8.2: Management support and risk assessment correlation analysis

		RA	MS
RA	Pearson Correlation	1	.804**
	Sig. (2-tailed)		.000
	N	308	307
MS	Pearson Correlation	.804**	1
	Sig. (2-tailed)	.000	
	N	307	309

The findings showed that there was a positive correlation between management support and risk assessment [r = 0.804, n = 307, p = 0.000]. With $p < 0.05$, this correlation is statistically significant with high scores for management support associated with high scores for risk assessment.

8.2.1.1 Interpretation of the management support and risk assessment correlation

As discussed in Chapter 7, the findings revealed that risk assessment was the most important construct of all the constructs of the framework proposed. As shown in the proposed framework, the risk assessment is the first step on which an organisation needs to embark in order to identify the threats, vulnerabilities and risks that must be mitigated. At this stage, the involvement of management is of the utmost importance.

Based on the results emanating from the risk assessment stage, it is recommended that management conducts a cost-benefit analysis of the implementation of the recommended controls aimed at reducing the risks which have been identified to an acceptable level. The BusinessDictionary (2001) defines a cost-benefit analysis as a "process of quantifying costs and benefits of a decision, program, or project (over a certain period), and those of its alternatives (within the same period), in order to have a single scale of comparison for unbiased evaluation". Should management decide that it is worthwhile to implement the recommended controls and the envisaged costs are within the budget, the risk assessment plan will be approved and the next phase of the policy construction may commence. If not, either the risk mitigation strategies will have to be revised so that they are within budget or the budget will have to be increased.

8.2.2 Management support and the information security policy construction correlation analysis

As depicted in Table 8.3, Pearson's correlation coefficient was used to investigate the relationship between management support and the information security policy construction.

Table 8.3: Management support and the information security policy construction correlation analysis

		MS	ISPC
MS	Pearson Correlation	1	.765**
	Sig. (2-tailed)		.000
	N	309	307
ISPC	Pearson Correlation	.765**	1
	Sig. (2-tailed)	.000	
	N	307	308

The findings show that there was a positive correlation between management support and information security policy construction [r=0.765, n = 307, p = 0.000]. With $p < 0.05$, this correlation is statistically significant with high scores for management support associated with high scores for information security policy construction.

8.2.2.1 Interpretation of the management support and information security policy construction correlation

As discussed in Chapter 6, it is imperative that the construction of an information security policy start with top management. The directives or high level security policies emanating from the executive management are then disseminated from the strategic level to the tactical level where they are translated into standards or guidelines and, finally, to the operational level as procedures (Von Solms et al., 2011). During the information security construction stage, management involvement is essential because management needs to approve the security policy. As discussed in Chapter 6 (Figure 6.6 depicting the flow chart diagram of information security policy construction), if management approves the security policy, the next stage involves the publication of the policy. On the other hand, if management does not approve the policy, the security policy team will have to incorporate management's recommendations into the existing policy and resubmit the policy to management for approval.

Furthermore, during the survey, the respondents were asked to indicate the importance of the following statement which is linked to management involvement in the security policy development: *Executive management is involved in the whole process of information security policy development*. The respondents agreed on the importance of the management involvement in security policy development with a 37.7% of the respondents agreeing that it was very important; 37.0% that it was important; 18.5% were neutral; 5.8% agreed it was somewhat important, while 1.0% stated that it was not important.

8.2.3 Management support and information security policy implementation correlation analysis

As depicted in Table 8.4, Pearson's correlation coefficient was used to investigate the relationship between management support and the information security policy implementation constructs.

Table 8.4: Management support and the information security policy implementation correlation analysis

		MS	ISPI
MS	Pearson Correlation	1	.673**
	Sig. (2-tailed)		.000
	N	309	306
ISPI	Pearson Correlation	.673**	1
	Sig. (2-tailed)	.000	
	N	306	307

It was found that there was a moderate positive correlation between management support and information security policy implementation [r=0.673, n = 306, p = 0.000]. With $p < 0.05$, this correlation is statistically significant with high scores for management support associated with high scores for information security policy implementation.

8.2.3.1 Interpretation of management support and the information security policy implementation correlation

During the information security policy implementation stage, the policies are rolled out throughout the entire organisation. Chapter 6 revealed that this stage includes the following four factors, namely, information security policy awareness; information security policy training; role of stakeholders and information security policy education. Management support is crucial in the information security policy implementation stage and it is incumbent on top management to formulate a communication plan to be

disseminated to all the various organisational levels. A high degree of participation on the part of management will motivate employees to comply with the new policy requirements.

This, in turn, will increase the security policy acceptance as well as the employees' commitment to the organisation's policies. In addition, management plays a significant role in the information security awareness and management needs to make sure that all the stakeholders are aware of and understand their responsibilities in respect of the security policy requirements. In order to reach such audiences, various business communication modes (notices, intranet, posters, newsletters, etc.) may be used to promote the security policy awareness. Furthermore, management must ensure that there are mechanisms in place to train and educate users on the new information security policy requirements. These may be organised either periodic or non-periodic based on the needs of the training and education sessions. In order to accomplish the information security policy training and education, management must ensure that they have sufficient budget allocated for the running of these sessions.

8.2.4 Management support and the information security policy monitoring and review correlation analysis

Table 8.5 presents the results of the Pearson's correlation coefficient that was used to investigate the relationship between management support and the information security policy monitoring and review construct.

Table 8.5: Management support and the information security policy monitoring and assessment correlation analysis

		MS	ISPM
MS	Pearson Correlation	1	.669**
	Sig. (2-tailed)		.000
	N	309	306
ISPM	Pearson Correlation	.669**	1
	Sig. (2-tailed)	.000	
	N	306	307

The findings show that there was a moderate positive correlation between management support and information security policy monitoring [r=0.669, n = 306, p = 0.000]. With $p < 0.05$, this correlation is statistically significant with high scores for management support associated with high scores for the information security policy monitoring and assessment construct.

8.2.4.1 Interpretation of management support and the information security policy monitoring and review correlation

Management plays a significant role in the information security policy monitoring and assessment stage. Management is responsible for the well-being of the organisation and, thus, it is essential that management is aware of the prevailing state of the organisation's information security. In the Direct-Control Cycle proposed by Von Solms et al. (2011), they emphasise the importance of the controlling step. Von Solms et al. (2011) state "in order to effectively control, it is necessary to capture data to test for compliance with the policies which were drafted and implemented through directing. At the operational level, this data could be extracted from, for example, log files of operating systems, databases and firewalls". Chapter 6 presented a discussion of both the monitoring and reviewing of the audit trails and automated reviews. The information acquired from these files must be compiled into a report and submitted to management. Thereafter management should assess such reports and make decisions accordingly.

8.2.5 Management support and the information security policy compliance correlation analysis

As depicted in Table 8.6, Pearson's correlation coefficient was used to investigate the relationship between management support and the information security policy compliance constructs.

Table 8.6: Management support and the information security policy compliance correlation analysis

		MS	ISPCO
MS	Pearson Correlation	1	.654**
	Sig. (2-tailed)		.000
	N	309	306
	Pearson Correlation	.654**	1
	Sig. (2-tailed)	.000	
	N	306	307

The findings show that there was a moderate positive correlation between management support and information security policy compliance [r=0.654, n = 306, p = 0.000]. With $p < 0.05$, this correlation is statistically significant with high scores for management support associated with high scores for information security policy compliance.

8.2.5.1 Interpretation of management support and the information security policy compliance correlation

During the survey, the respondents were asked to indicate the importance of the following statement which is linked to management involvement in the security policy enforcement: *The involvement of executive management in the information security policy development is crucial to the approval of the security policies*. The respondents agreed on the importance of the management involvement in security policy enforcement with a 31.1% of the respondents agreeing that it was very important; 38.4% that it was important; 20.7% were neutral; 6.2% agreed it was somewhat important, while 1.6% stated that it was not important.

Once the information security policy has been implemented in the organisation and the employees have been trained and are aware of the organisation's information security policy, it is essential that management put in place appropriate measures to ensure information security policy compliance. Such measures will check whether the information security policies' requirements are being met. In order to understand the behaviour of employees in respect of security policies, Chapter 6 recommended using existing theories related to information security policy compliance such as Theory of Planned Behaviour and General Deterrence Theory.

8.2.6 Management support and the employee support correlation analysis

As depicted in Table 8.7, Pearson's correlation coefficient was used to investigate the relationship between management support and the employee support constructs.

Table 8.7: Management support and the employee support correlation analysis

		MS	ES
MS	Pearson Correlation	1	.680**
	Sig. (2-tailed)		.000
	N	309	308
ES	Pearson Correlation	.680**	1
	Sig. (2-tailed)	.000	
	N	308	309

The findings showed a positive correlation between management support and employee support [r=0.680, n = 308, p = 0.000]. With $p < 0.05$, this correlation is statistically

significant with high scores for management support associated with high scores of employee support.

8.2.6.1 Interpretation of management support and the employee support correlation

The successful implementation of an effective information security policy depends on sound cooperation between management and employees. Management is in charge of an organisation's activities and it is vital that management demonstrates a sound managerial leadership style in order to motivate employees to adhere to organisational policies. If management demonstrates acceptable behaviour as regards adhering to the information security policy then it is likely that employees will also demonstrate acceptable behaviour and comply with the information security policy.

8.3 Correlation analysis between employee support and the Information Security Policy Development Life Cycle (ISPDLC)

Objective: Investigate the relationship between employee support and the ISPDLC constructs.

Based on the proposed framework it may be argued that employee support is important in all the steps of the ISPDLC. Accordingly, a statistical test was conducted to ascertain whether employee support is statistically related to the ISPDLC constructs.

8.3.1 Employee support and risk assessment correlation analysis

As shown in Table 8.8, Pearson's correlation coefficient was used to investigate the relationship between employee support and risk assessment constructs.

Table 8.8: Employee support and risk assessment correlation analysis

		MS	ES
MS	Pearson Correlation	1	.756**
	Sig. (2-tailed)		.000
	N	309	307
ES	Pearson Correlation	.756**	1
	Sig. (2-tailed)	.000	
	N	307	308

The findings showed a positive correlation between employee support and risk assessment [r=0.756, n = 307, p = 0.000]. With $p < 0.05$, this correlation is statistically significant with high scores for employee support associated with high scores of risk assessment.

8.3.1.1 Interpretation of the employee support and risk assessment correlation

As discussed in Chapter 3, the employees who work within an organisation constitute the major threat to the organisation's information security. Accordingly, the involvement of employees in the risk assessment process is crucial. It was pointed out in Chapter 6 that organisations need both to identify the assets to be protected and to assess the threats and vulnerabilities during the risk assessment stage. Thus, employees need to be involved in the assets identification. For example, such assets include the computers that are used by employees and, thus, it is incumbent on employees to cooperate with the staff members who are involved in these activities. Such cooperation is also necessary during the threats and vulnerability identification process.

8.3.2 Employee support and information security policy construction correlation analysis

As depicted in Table 8.9, Pearson's correlation coefficient was used to investigate the relationship between employee support and information security policy construction.

Table 8.9: Employee support and information security policy construction correlation analysis

		ES	ISPC
ES	Pearson Correlation	1	.731**
	Sig. (2-tailed)		.000
	N	309	307
ISPC	Pearson Correlation	.731**	1
	Sig. (2-tailed)	.000	
	N	307	308

The results showed that there was a positive correlation between employee support and information security policy construction [r=0.731, n = 307, p = 0.000]. With $p < 0.05$, this correlation is statistically significant with high scores for employee support associated with high scores for information security policy construction.

8.3.2.1 Interpretation of the employee support and information security policy construction correlation

It was argued in Chapter 6 that employees should be involved in the construction of an information security policy in order to create a sense of ownership on the part of employees as regards the information security policy. In addition, it is critical at this stage to start preparing the employees for the upcoming changes in the ways in which they will have to operate once the new policy requirements have been implemented. The involvement of employees is critical in moving the users through the stages of commitment from preparation through acceptance and, ultimately, to the commitment stage.

8.3.3 Employee support and information security policy implementation correlation analysis

Table 8.10 presents the results of the Pearson's correlation coefficient that was used to investigate the relationship between employee support and information security policy implementation.

Table 8.10: Employee support and information security policy implementation correlation analysis

		ES	ISPI
ES	Pearson Correlation	1	.717**
	Sig. (2-tailed)		.000
	N	309	306
ISPI	Pearson Correlation	.717**	1
	Sig. (2-tailed)	.000	
	N	306	307

The results showed that there was a positive correlation between employee support and information security policy implementation [r=0.717, n = 306, p = 0.000]. With $p < 0.05$, this correlation is statistically significant with high scores for employee support associated with high scores of information security policy implementation.

8.3.3.1 Interpretation of the employee support and information security policy implementation correlation

During the implementation of new information security policies it is imperative that employees are involved. In Chapter 6 it was emphasised that employees should formally

sign the new information security policy to ensure that the new information security policy document is a binding contractual agreement between the employers and the employees. The contract should include rules that the employees must abide by in order to protect the organisation's information assets as well as stipulating the penalties that will be imposed on the employees should they violate the policy's requirements.

In addition, employees must be required to attend training and education programmes in order to ensure that they understand the requirements of the policy. The main objective of such programmes is to increase the employees' knowledge about the policy requirements. Based on the Theory of Planned Behaviour, Chapter 6 discussed that "an employee's judgment of his/her own knowledge in complying with the requirements of the information security policy positively influences his/her intention to comply with the requirements of the information security policy" (Bulgurcu et al., 2010).

8.3.4 Employee support and the information security policy monitoring and review correlation analysis

Table 8.11 presents the results of Pearson's correlation coefficient that was used to investigate the relationship between employee support and information security policy monitoring and review constructs.

Table 8.11: Employee support and the information security policy monitoring and review correlation analysis

		ES	ISPM
ES	Pearson Correlation	1	.741**
	Sig. (2-tailed)		.000
	N	309	306
ISPM	Pearson Correlation	.741**	1
	Sig. (2-tailed)	.000	
	N	306	307

It was found that there was a positive correlation between employee support and information security policy monitoring [r=0.741, n = 306, p = 0.000]. With $p < 0.05$, this correlation is statistically significant with high scores for employee support associated with high scores for information security policy monitoring and review.

8.3.4.1 Interpretation of the employee support and information security policy monitoring and assessment correlation

As highlighted in Chapter 6, one of the objectives of information security policy monitoring and assessment is to produce measurable results that provide evidence of the users' behaviours. The results of such monitoring and assessment should be used to assess the employees' performance in terms of security policy compliance. During the audit of security policy compliance, employees who demonstrate a high degree of security policy compliance should be encouraged and rewarded (Talbot and Woodward, 2009). On the other hand, those who are found to be violating the organisation's policies should be cautioned and penalised (Diver, 2007).

8.3.5 Employee support and information security policy compliance correlation analysis

As depicted in Table 8.12, Pearson's correlation coefficient was used to investigate the relationship between employee support and information security policy compliance.

Table 8.12: Employee support and information security policy compliance correlation analysis

		ES	ISPM
ES	Pearson Correlation	1	.774**
	Sig. (2-tailed)		.000
	N	309	306
ISPM	Pearson Correlation	.774**	1
	Sig. (2-tailed)	.000	
	N	306	307

It emerged that there was a positive correlation between employee support and information security policy compliance [r=0.774, n = 306, p = 0.000]. With $p < 0.05$, this correlation is statistically significant with high scores for employee support associated with high scores for information security policy compliance.

8.3.5.1 Interpretation of the employee support and information security policy compliance correlation

In Chapter 6 it was argued that organisations need to rely on existing theories related to information security policy compliance in order to understand employees' intentions to comply with the information security policy. Based on Theory of Planned Behaviour, it was argued that an employee's intention to comply with the organisation's information

security policy is related to the employee's attitude to compliance, normative beliefs and perceived behavioural control. In addition, this study states that deterrence measures reduce the risk of employees intentionally violating the organisation's information security policies. However, employees should not consider security policies as a tool of punishment tool but rather as security measures that will help to protect the organisation's assets and thereby grow the organisation's business. The next section concludes this chapter.

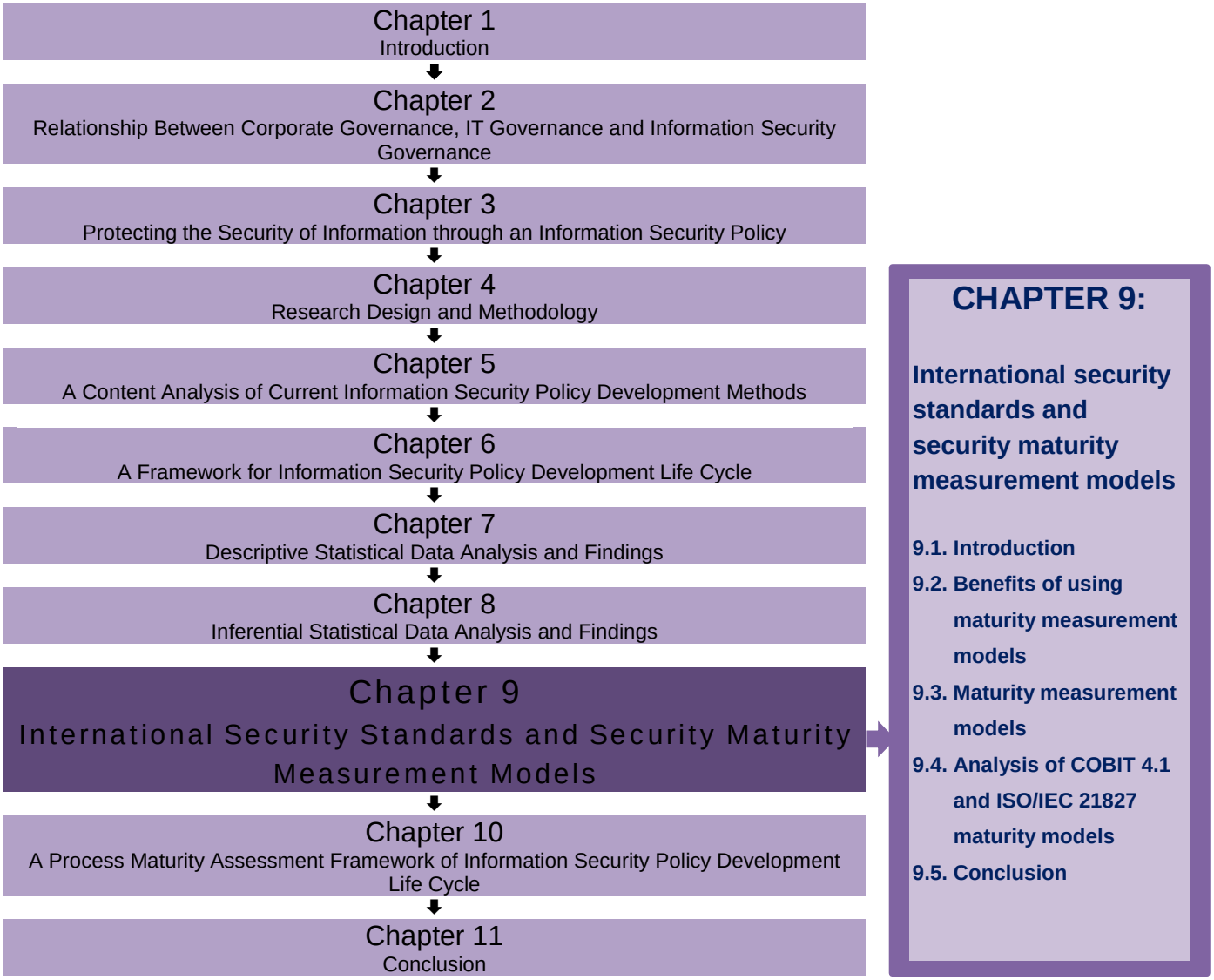
8.4 Conclusion

A key assumption made in Chapter 7, in which the framework of this study was discussed, was that it is essential that there be management support as regards all the ISPDLC processes, namely, risk assessment; information security policy construction; information security policy implementation; information security policy monitoring and information security policy compliance. This chapter discussed the statistical tests that were conducted to ascertain whether there is was relationship between management support and ISPDLC constructs. The findings showed a positive correlation between management support and the ISPDLC constructs with a statistically significant result. Accordingly, the findings confirmed the assumption that had been made. The results were then applied to the proposed framework. It emerged that, as management support increased/decreased, a concomitant increase/decrease could be expected in the ISPDLC constructs. For example, a high degree of involvement on the part of management, for example, voting sufficient budget for the risk assessment process, would result in the success of the information security policy construction process.

The assumption was also made that there needs to be employee support in respect of all the ISPDLC constructs. This chapter described the statistical tests that were conducted to ascertain whether there was a relationship between employee support and the ISPDLC constructs. The findings confirmed the existence of a significant relationship between employee support and the ISPDLC constructs. In other words, as employee support increased/decreased, an increase/decrease could be expected in the ISPDLC constructs. For example, a high degree of employee support, such as the participation in information security policy training, education and awareness sessions, would result in the success of the information security policy implementation process.

This Chapter highlights the relationship between management, employee support and the ISPDLC constructs. The next Chapter will discuss the international security standards and security maturity models.

Chapter 9: International Security Standards and Security Maturity Measurement Models



9.1 Introduction

The current literature concentrates on the assessment of information security policies based on their content and structure (Grobler, 2008; Mlangeni and Biermann, 2005; Goel and Chengalur-Smith, 2010; Doherty et al., 2009). The study conducted by Goel and Chengalur-Smith (2010) assessed information security policy based on the three dimensions (breadth, clarity and brevity) that could be used to identify how well a security policy is written. To the researcher's knowledge, there is no comprehensive empirical study that has targeted the assessment of the information security development life cycle.

This study states that the evaluation of the processes involved in the development of security policies is critical to improving security policy quality. Accordingly, the focus of this chapter is to integrate security maturity assessment into the security policy development using a maturity model approach. This chapter investigates existing theories and maturity models in order to ascertain the best approach that organisations should adopt in order to assess the processes of developing and implementing an effective information security policy. ISO/IEC 21827: Systems Security Engineering – Capability Maturity Model Capability Maturity Model and the Control Objectives for Information and Related Technology (COBIT) security maturity models were chosen to guide this assessment. In addition, the chapter contains a comparison between the COBIT domains and the ISO/IEC 21827 (2008) process areas in order to gain an insight into the key criteria that should be used to assess the maturity levels of the information security policy development life cycle.

9.2 Benefits of using maturity measurement models

Before discussing the benefits of maturity models, it is important to understand what a maturity model is. Okongwu, Morimoto, and Lauras (2013, p. 8) define a maturity model "as a structured collection of elements that describe the characteristics of effective processes at different stages of development. It also suggests points of demarcation between stages and methods of transitioning from one stage to another.''

According to Becker, Knackstedt, and Pöppelbu (2009, p. 11), ''a maturity model consists of a sequence of maturity levels for a class of objects. It represents an anticipated, desired, or typical evolution path of these objects shaped as discrete stages. Typically, these objects are organisations or processes.'' The common feature in these two definitions is the fact that that a maturity model represents different stages or levels that specify whether a number of processes have been accomplished.

Chapin and Akridge (2005) and Eshlaghy and Pourebrahimi (2011) state that implementing a security maturity model in an organisation enables the organisation to:

- generate reproducible and valid measurements,
- establish actual progress in the security milieu,
- rank itself against a range of organisations,
- determine the order in which security controls should be applied,
- determine the resources required to apply to the security programme.

The above mentioned highlights the fact that implementing a maturity model enables the organisation concerned to benchmark itself against other organisations. This, in turn, will enable the organisation to work out the areas in which it is either underperforming or not performing. In addition, a maturity model enables the security controls to be coordinated during the implementation (Abu-Khadra, Chan, and Pavelka, 2012).

Man (2007) argues that the use of a maturity model is important because it helps the organisation to keep track of the activities and best practices which have been accomplished and categorise these activities into a progressive level of maturity. A security maturity model indicates both the degree of development and the strength of the organisation's security measures (Eshlaghy and Pourebrahimi, 2011). According to Man (2007), the main benefit of implementing a maturity model becomes evident when an organisation has finished evaluating its current practices and wishes to advance to the desired level of maturity. Once the organisation has conducted a maturity assessment, it is able to compare its current activities with the activities specified in the maturity model. This, in turn, enables the organisation to ascertain its own strengths and weaknesses, thus assisting the organisation to prioritise its actions to order to effect improvements. The next section discusses examples of existing maturity models discussed in the literature.

9.3 Maturity measurement models

This research project used the ISO/IEC 21827 and COBIT 4.1 security standards to guide the maturity assessment of the information security policy development and implementation process. The COBIT and ISO/IEC 21827 maturity models were chosen because they are recognised international standards. In addition, they are information security based and are widely accepted by both practitioners and academics (Abu-

Khadra et al., 2012). COBIT was chosen because it is a generic framework and, thus, it does not focus specifically on a particular organisation (COBIT, 2007). Abu-Khadra et al. (2012) maintain that COBIT "is a framework of generally applicable IS security and control practices for information technology control systems."

ISO/IEC 21827 describes the security processes that an organisation should follow throughout the entire system development life cycle. ISO/IEC 21827 (2008, p. 42) states that "security engineering, like other engineering disciplines, is a process that proceeds through concept, design, implementation, test, deployment, operation, maintenance and decommission". This research project adopted the same concept as it investigated the processes of the information security policy development life cycle.

In addition to COBIT and ISO/IEC 21827, there are other maturity models mentioned in the literature that may be used to measure the maturity of diverse aspects of information technology and information security. These maturity models are briefly described in the section below:

9.3.1 Cyber Security Capability Maturity Model

The Cyber Security Capability Maturity Model (C2M2) encompasses four scales of Maturity Indicator Levels (MILs), from 0 to 3 (C2M2, 2014). The model is organised into the following 10 domains, namely, 1. Risk management; 2. Asset, change and configuration management; 3. Identity and access management; 4. Threat and vulnerability management; 5. Situational awareness; Information sharing and communications; 6. Event and incident response; 7. Continuity of operations; 8. Supply chain and external dependencies management; 9. Workforce management, and 10. Cyber security programme management. The C2M2 focuses on the implementation and management of those cyber security practices that are related to both information technology (IT) and operation technology assets (C2M2, 2014).

9.3.2 Information Security Management System Maturity Model

The Information Security Management System (ISMS) Maturity Model was proposed by Woodhouse (2008). Woodhouse (2008) argued that the existing security maturity models did not define a maturity assessment which was less than one. The ISMS describes nine levels of process maturity, four of which are below the existing five levels defined in most of the popular models. The levels are subdivided into two categories, namely, managed processes which encompass levels one to five, and unmanaged processes which are

below level 1. The managed processes include the functional, technical, operational, managed, and strategic while the unmanaged processes include the negligent, obstructive, arrogant and subversive (Woodhouse, 2008). The ISMS maturity model focuses on both cultural issues and process integration (Woodhouse, 2008).

9.3.3 IBM – Information Security Framework

IBM – Information Security Framework (IBM-ISF) was developed by IBM (2007). The model is composed of five maturity levels namely: 1. Initial, 2. Basic, 3. Capable 4. Efficiency, and 5. Optimising. The IBM-ISF focuses on the security gap analysis (IBM, 2007).

9.3.4 Citigroup's Information Security Evaluation Model

The Citigroup's Information Security Evaluation Model (Citi-ISEM) was proposed by Citi-ISEM (2000). The model comprises five maturity levels, namely, 1. Complacency 2. Acknowledgement 3. Integration 4. Common practice and 5. Continuous improvement. The model focuses on the security awareness, adoption and evaluation of organisations (Citi-ISEM, 2000).

9.3.5 Gartner's Information Security Awareness Maturity Model

Gartner's Information Security Awareness Maturity Model (GISMM) was proposed by (Dzazali et al., 2009). The model comprises four maturity levels, namely, 1. Blissful ignorance 2. Awareness 3. Corrective and 4. Operations Excellence. GISMM focuses on security awareness and risk management. The next section discusses the maturity models selected, namely, COBIT 4.1 and ISO/IEC 21827.

9.4 Analysis of the COBIT 4.1 and ISO/IEC 21827 maturity models

The ISO/IEC 21827 process areas and maturity levels are explored in this chapter as are the domains and maturity levels of COBIT 4.1. The chapter then compares their processes and maturity levels. The result provides the optimum approach that should be followed when measuring the process of developing and implementing an effective information security policy in an organisation.

9.4.1 History of ISO/IEC 21827

The Capability Maturity Model (CMM) was developed by the Software Engineering Institute (SEI) at Carnegie- Mellon University in 1986 (CMM, 2003). The project was funded by the Department of Defence of the United States of America. The model was developed in order to find a solution to the problem of the productivity and quality of software applications projects (Lutteroth, Reilly, Dobbie, and Hamer, 2007). At that time, projects were either not able to meet deadlines and were running out of budget with this resulting in complete failure (SSE-CMM, 2003). The SSE-CMM's objectives included evolving security engineering into a mature and quantifiable discipline which enabled focused investments (SSE-CMM, 2003).

"The idea behind CMM is that a high-quality process yields a high-quality product at the end" (Lutteroth et al., 2007). In 1996, SSE-CMM version 1.0 was published with version 2.0 becoming available in 1999. In 2002, SSE-CMM was adopted as the international standard known as ISO/IEC 21827. The International Standard Organisation (ISO) published a revised version of ISO/IEC 21827 in 2008. This revised version included greater detail on incorporating measurement activities into the SSE-CMM as compared to the previous version (ISO/IEC 21827, 2008). This research project will refer to the revised version.

9.4.1.1 Structure of ISO 21827

The ISO/IEC 21827 (2008) includes 22 Process Areas (PAs). These PAs are considered to be the fundamental parts of the majority of, if not all, activities. A process area is "a defined set of related process characteristics, which when performed collectively, can achieve a defined purpose" (SSE-CMM, 2003). The PAs themselves are divided into a number of parts which are known as the Base Practices (BPs). SSE-CMM specifies 129 base practices which are organised into 22 PAs. A base practice is the activity that must be accomplished in order to satisfy the requirement of a particular process area (ISO/IEC 21827, 2008). The 22 PAs are subdivided into 11 security engineering process areas and 11 project and organisational process areas.

These PAs are themselves divided into a number of parts which are known as base practices (BPs). It specifies 129 base practices which are organised into 22 process areas. The 22 PAs are subdivided into 11 security engineering process areas and 11 project and organisational process areas. Each PA has a set of goals which are achieved through performing the base practices pertaining to that specific process area. These

process areas are numbered in no particular order because the SSE-CMM does not specify a specific process or the sequence of the process's implementation. The process areas of the security engineering domain are specifically organised to meet a broad spectrum of security engineering needs (SSE-CMM, 2003). Table 9.1 presents the objectives of the security engineering process areas. These objectives are taken directly from ISO/IEC 21827.

Table 9.1: Security engineering process areas

PA No.	Process area	Goal
PA 01	Administer Security Control	"Ensure that the intended security is achieved in its operational state".
PA 02	Assess Impact	"To identify the likelihood of the impacts occurring".
PA 03	Assess Security Risk	"To identify, analyse and evaluate the security risks".
PA 04	Assess Threat	"To identify security threats and their properties".
PA 05	Assess Vulnerability	"To identify and characterize system security vulnerabilities".
PA 06	Build Assurance Argument	"To clearly convey that the customer's security needs are met".
PA 07	Coordinate Security	"To ensure that all parties are aware of and involved with security".
PA 08	Monitor Security Posture	"To ensure that all breaches of security are identified and reported".
PA 09	Provide Security Input	"To provide users with the security information they need".
PA 10	Specify Security Needs	"To identify the needs related to security for the system".
PA 11	Verify and Validate Security	"To ensure that solutions are verified and validated with respect to security".

In addition to the 11 security engineering process areas, ISO/IEC 21827 encompass 11 project and organisational areas as illustrated in Table 9.2**.**

Table 9.2: Project and organisational process areas

PA No.	Process Area	Goal
PA 12	Ensure quality	"To ensure the quality of the system and the quality of the process being used to create the system and the degree to which the project follows the defined process".
PA 13	Manage configuration	"To maintain data on and the status of identified configuration units, and to analyze and control changes to the system and its configuration units".
PA 14	Manage project Risk	"To identify, assess, monitor, and mitigate risks to the success of both the systems engineering activities and the overall technical effort".
PA 15	Monitor and control technical effort	"To provide adequate visibility of actual progress and risks".

PA No.	Process Area	Goal
PA 16	Plan technical effort	"To establish plans that provide the basis for scheduling, costing, controlling, tracking, and negotiating the nature and scope of the technical work involved in system development".
PA 17	Define organisation's systems	"To create and manage the organisation's standard systems engineering processes".
PA 18	Improve organisation's systems	"To gain competitive advantage by continuously improving the effectiveness and efficiency of the systems processes".
PA 19	Manage product line evolution	"To introduce services, equipment, and new technology to achieve the optimal benefits in product evolution".
PA 20	Manage systems support environment	"To provide the technology environment needed to develop the product and perform the process".
PA 21	Provide on-going skills	"To ensure that projects and the organisation have the necessary knowledge and skills to achieve project and organisational objectives".
PA 22	Coordinate with suppliers	"To address the needs of organisations to effectively manage the portions of product work that are conducted by other organisations".

The 22 security engineering and project and organisational process areas presented in Tables 9.1 and 9.2 are numbered in no particular order because the SSE-CMM does not specify a specific process or sequence. The process areas of the security engineering domain are specifically organised to meet a broad spectrum of security engineering needs (SSE-CMM, 2003). In view of the nature of this research project, the 11 security engineering process areas only will be used to formulate a maturity model for assessing the information security policy development and implementation.

9.4.1.2 Security engineering process

ISO/IEC 21827 divides the security engineering into three major areas: **risk**, **engineering** and **assurance**. The risk process identifies and prioritises possible threats to the system. In order to mitigate the identified threats, the engineering process collaborates with other engineering disciplines in order to implement appropriate solutions (SSE-CMM, 2003). The assurance process establishes confidence in the solutions and communicates it to the customers. Figure 9.1 depicts the three security engineering categories diagrammatically.

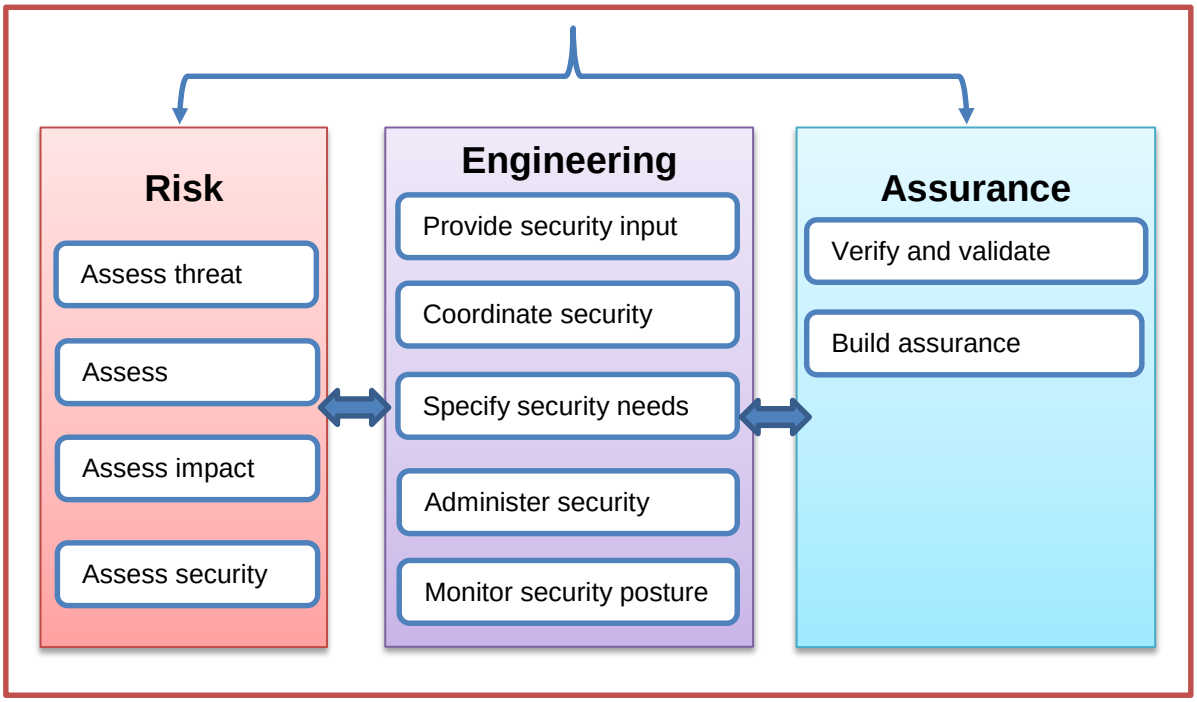


Figure 9.1: Three main areas of security engineering process (SSE-CMM, 2003)

In order to obtain the requisite risk information, ISO/IEC 21827 (2008) recommends that organisations conduct the following processes: PA04 (Assess threat); PA05 (Assess vulnerability); PA02 (Assess impact) and, finally, PA03 (Assess security risk). Security engineering includes the following process areas: PA01 (Administer security control), PA07 (Coordinate security), PA08 (Monitor security posture), PA09 (Provide security input) and PA10 (Specify security needs). Thus the security engineering category describes the essential features of an organisation's security engineering process that must exist in order to ensure good security engineering.

The last category is the assurance category. The Oxford Dictionary (2001) defines assurance as "a positive declaration intended to give confidence or a promise." Assurance is concerned with making sure that the organisation's stakeholders are confident that the system is working properly and as intended. The build assurance argument PA identifies the base practices that address the collecting of measurements and other data to prove that the system security engineering claims about the system are evident.

The ISO/IEC 21827 standard includes the following security engineering practices:

- "the entire life cycle, including development, operation, maintenance and decommissioning activities;

- the whole organisation, including management, organisational and engineering activities;
- concurrent interactions with other disciplines, such as system, software, hardware, human factors and test engineering; system management, operation and maintenance;
- interactions with other organisations, including acquisition, system management, certification, accreditation and evaluation" (ISO/IEC 21827, 2008).

The next section discusses the COBIT 4.1.

9.4.2 COBIT 4.1

COBIT was created in 1992 by the Information Systems Audit and Control Association (ISACA) and the IT Governance Institute (ITGI). COBIT first edition was published in 1996 with the second edition becoming available in 1998. The third edition was released in 2000 and the on-line edition became available in 2003. The fourth edition of COBIT was issued in December 2005. After the amendments to COBIT 4.0, ITGI released an update of COBIT 4.1 version in 2007. COBIT 4.1 is "an IT Governance framework and supporting tool set that allows managers to bridge the gap between control requirements, technical issues and business risks" (ITGI, 2005, p. 22).

The COBIT maturity model focuses on governance and auditing specific procedures. COBIT encompasses 34 processes which are subdivided into 4 domains: Plan and Organise (PO), Acquire and Implement (AI), Deliver and Support (DS) and Monitor and Evaluate (ME) (COBIT, 2007).

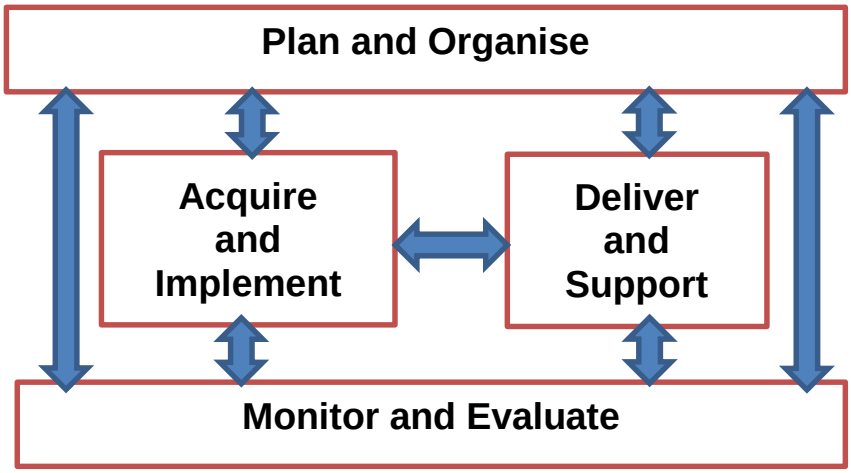


Figure 9.2: The four interrelated domains of COBIT (COBIT, 2007)

- **Plan and Organise (PO):** This domain covers strategy and tactics, as well as the identification of the way in which IT may best contribute to the achievement of the business objectives (COBIT, 2007).

- **Acquire and Implement (AI):** This domain emphasises that in order to realise the IT strategy, IT solutions need to be identified, developed or acquired, as well as implemented and integrated into the business process (COBIT, 2007).

- **Deliver and Support (DS):** This domain is concerned with the actual delivery of the required services and which includes service delivery, management of security and continuity of business support, service support for users, and management of data and operational facilities (COBIT, 2007).

- **Monitor and Evaluate (ME):** All IT processes need to be regularly assessed over time for their quality and compliance with control requirements. Accordingly, this domain addresses performance management, monitoring of internal control, regulatory compliance and governance (COBIT, 2007).

In the next section, the 34 COBIT processes are mapped with the 11 SSE-CMM security engineering process areas.

9.4.3 Mapping COBIT domains and SSE-CMM process areas

A study conducted by Ahuja and Goldman (2009) explored the mapping of COBIT's four domains processes area with SSE-CMM's 22 process areas. The main objective of the study was to integrate COBIT, SSE-CMM and Balanced Scorecard (BSC) in order to formulate a comprehensive strategic information security management process (Ahuja and Goldman, 2009). During the mapping, COBIT's fifth domain of delivery and support (DS 5), which ensures system and security, was expanded because the focus was on the security based. A high-level mapping of the other three domains was accomplished. Table 9.3 depicts the mapping of the COBIT domains with the SSE-CMM process areas.

Table 9.3: SSE-CMM and COBIT mapping (Ahuja and Goldman, 2009)

COBIT Domains	SSE-CMM Process Areas (PA) and Base Practices (BP) high level correlation
Plan and Organize (PO)	
PO1 – PO 11	Managed by Business/IT Alignment
AI 1 – AI 6	Managed by organisational processes
Deliver and Support (DS)	
DS1 Define and Manage service levels	PA 01 (BP: 1-4)
DS2 Manage third party services	PA 12 – PA 22
DS3 Manage performance and capacity	PA 12 – PA 22
DS4 Ensure continuous service	PA 12 – PA 22
DS5 Ensure systems security	
5. 1 Management of IT Security	PA 01 (BP: 1-4), PA 02 (BP: 1-6), PA 03 (BP: 1-6), PA 04 (BP: 1-6), PA 05(BP: 1-5)
5. 2 IT security plan	PA 06(BP: 1-5), PA 10(BP: 1-7)
5. 3 Identity management	PA 01 – PA 11
5. 4 User account management	PA 01 – PA 11
5. 5 Testing, surveillance, monitoring	PA 06 (BP: 1-5), PA 08 (BP: 1-7)
5. 6 Security incident definition	PA 02 (BP: 1-6), PA 03 (BP: 1-6)
5. 7 Protection of security technology	PA 07 (BP: 1-4), PA 08 (BP: 1-7)
5. 8 Cryptographic key management	PA 01 – PA 11
5. 9 Prevention, detection and correction	PA 03 (BP: 1-6), PA 07 (BP: 1-4), PA 08 (BP: 1-7)
5. 10 Network Security	PA 01 – PA 11
DS6 Identify and allocate costs	PA 12 – PA 22
DS7 Educate and train users	PA 01 (BP: 3), PA 09 (BP: 5-6), PA 10 (BP: 2)
DS8 Assist and advise customers	PA 10 (BP: 1-7)
DS9 Manage configuration	PA 01 (BP: 1-4), PA 07 (BP: 1-4)
DS10 Manage incidents	PA 03 (BP: 1-6), PA 07 (BP: 1-4), PA 08 (BP: 1-7)
DS11 Manage data	PA 03 (BP: 1-6), PA 07 (BP: 1-4), PA 08 (BP: 1-7)
DS12 Manage facilities	PA 12 – PA 22
DS13 Manage Operations	PA 12 – PA 22
Monitor and Evaluate (ME)	
ME1 Monitor and Evaluate IT performance	PA 11 (BP: 1-5)
ME2 Assess internal control adequacy	PA 11 (BP: 1-5), PA 8 (BP: 1-7)
ME3 Ensure regulatory compliance	PA 10 (BP: 2), PA 06 (BP: 1-5), PA 11 (BP: 1-5)
ME4 Provide IT Governance	PA 11 (BP: 1-5), PA 03 (BP: 1-6)

The findings of the study revealed that the COBIT's DS 5 processes matched with the SSE-CMM's security engineering base practices which are covered in Process Areas PA 1 – PA 11 (see Table 9.3).

Mallette (2005) conducted a correlation analysis of SSE-CMM's Key Performance Areas (KPA) and COBIT processes in order to understand possible synergies between the two models in terms of project management processes. The comparison was based on

matching process key words, such as project plan, project tracking and oversight, quality management, audit, training, process documentation, configuration and change. The finding of the study revealed a significant correlation between the COBIT control objectives and the SSE-CMM practices. The next section discusses the maturity levels of the two international security standards.

9.4.4 ISO/IEC 21827 capability maturity levels

ISO/IEC 21827 (2008) describes maturity in terms of the capability levels of processes. The model encompasses five maturity levels: Initial, Repeatable, Defined, Managed and Optimized. Figure 9.3 graphically illustrates ISO/IEC 21827 maturity levels.

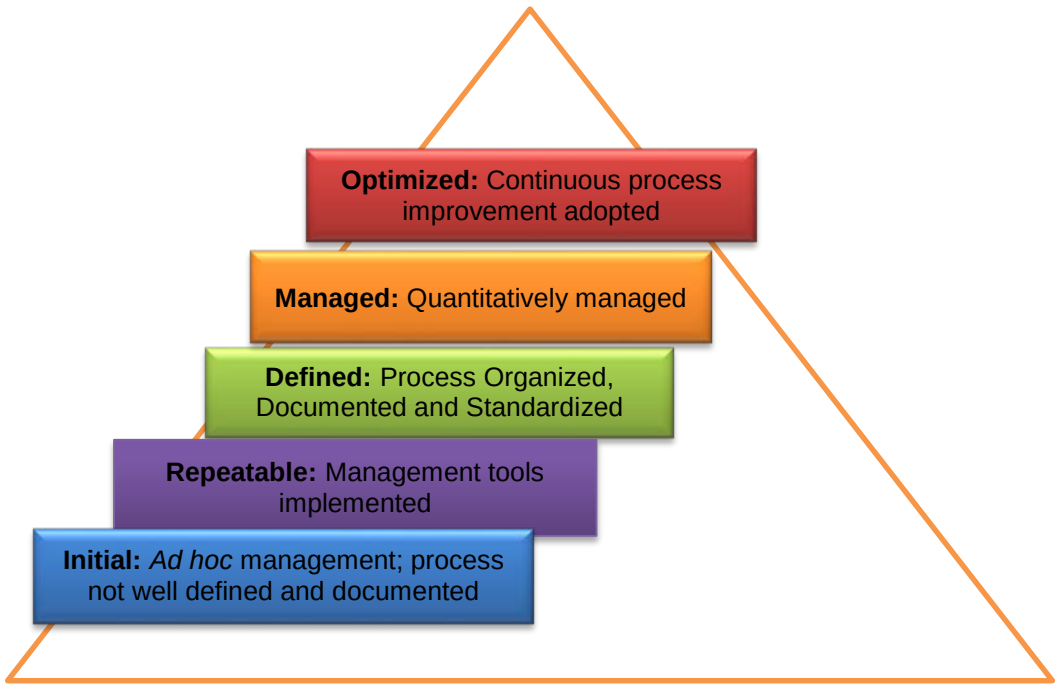


Figure 9.3: ISO/IEC 21827 maturity levels (ISO/IEC 21827, 2008)

ISO/IEC 21827 describes the stages through which processes progress as they are defined, implemented and improved. The higher the assessed level of maturity of the organisation, the better in theory the organisation is at defining, assessing and improving its process capability. The next section discusses COBIT's domains and maturity levels.

9.4.5 COBIT 4.1 maturity levels

COBIT 4.1 provides a maturity model component that enables executive management to assess and determine the maturity level of its internal control. COBIT 4.1 assesses the

capability of its maturity on five scales as described in Figure 9.4.5.1. ITGI (2005) states that for each of the predefined 34 IT processes, COBIT assists management to identify

- the actual performance of the enterprise: the current state
- the current status of the industry: for benchmarking purposes
- the enterprise's target for improvement: the desired state.

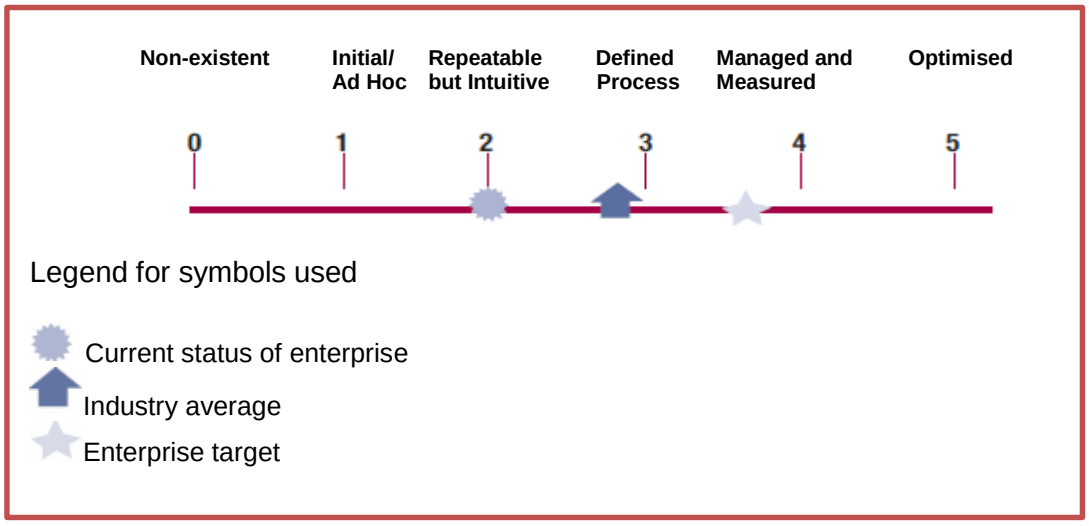


Figure 9.4: COBIT maturity levels (COBIT, 2007)

The five COBIT's maturity levels are discussed in the section below:

- **Maturity level 0 - Non-existent:** Management processes do not exist at all.
- **Maturity level 1 – Initial:** Processes are ad hoc and disorganised.
- **Maturity level 2 – Repeatable but intuitive:** Processes follow a regular pattern.
- **Maturity level 3 – Defined process:** Processes are documented and communicated.
- **Maturity level 4 – Managed and measurable:** Processes are monitored and measured.
- **Maturity level 5 – Optimised:** Good practices are followed and automated.

The next section describes the mapping of the five COBIT maturity levels with the five ISO/IEC 21827 maturity levels.

9.4.6 Mapping COBIT 4. 1 and ISO/IEC 21827 maturity levels

Table 9.4 depicts the mapping between COBIT 4.1 and ISO/IEC 21827 maturity levels. In addition, it shows the maturity criteria for each level.

Table 9.4: Mapping the COBIT 4.1 and ISO/IEC 21827 maturity levels

Maturity level	COBIT 4.1	ISO/IEC 21827	Maturity criteria
Level 0	**Non-existent:** • There is no recognition of the need for internal control. • Control is not part of the organisation's culture or mission		• No Process required
Level 1	**Initial / ad hoc:** • There is some recognition of the need for internal control. • The approach to risk and control requirements is ad hoc • Employees are not aware of their responsibilities	**Performed informally:** • Base practices of the process area are generally performed • The performance of these base practices may not be rigorously planned and tracked	• Need for internal control • Risk identification • Base practices performed
Level 2	**Repeatable but intuitive:** • Controls are in place but are not documented • Their operation is dependent on knowledge and motivation of individuals • Effectiveness is not adequately evaluated • Employees may not be aware of their responsibilities	**Planned and tracked:** • Base practices in the process area are planned and managed	• Controls identified • Control operation depends on individuals' knowledge • Process planned and managed
Level 3	**Defined:** • Controls are in place and are adequately documented • The evaluation process is not documented • Employees are aware of their responsibilities in respect of control	**Well defined:** • The process is planned and managed using an organisation-wide standard process • A standard process for the organisation is documented and describes how to implement the base practices of the process area	• Employees awareness • Controls are documented • Processes are implemented • Processes planned and managed
Level 4	**Managed and measurable:** • A formal, documented evaluation of controls occurs frequently • Controls are automated and regularly reviewed • Consistent follow-up to address identified control weakness	**Quantitatively managed:** • Detailed measures of performance are collected and analysed • Quantitatively understanding of the process capability	• Process evaluation • Processes are automated and reviewed • Processes are quantitatively understood
Level 5	Optimized: • Control evaluation is continuous based on self-assessments and gap and root cause analyses	**Continuously improving :** • Improvements to the standard process are identified • Defects produced are analysed in order to identify other potential enhancements to the standard process	• Controls evaluation • Process improvement • Defects analysed

The result of the mapping of the processes and maturity levels clearly shows that there is strong synergy between the two security models. Both COBIT and ISO/IEC 21827 include five maturity levels rating although COBIT starts with maturity level 0 which does not require any process. The COBIT maturity model is derived from the SSE-CMM

maturity model that the Software Engineering Institute defined for the maturity of software development capability (COBIT, 2007). COBIT (2007) points out that the difference between the SSE-CMM and COBIT maturity levels is their implementation. COBIT (2007) states that maturity levels are not designed for use as a threshold model in terms of which it is not possible to move to the next higher level without having fulfilled all the conditions of the lower level. COBIT (2007, p. 17) asserts that:

> "… in COBIT, a generic definition is provided for the COBIT maturity scale, which is similar to CMM but interpreted for the nature of COBIT's IT management processes. The scales should not be too granular, as that would render the system difficult to use and suggest a precision that is not justifiable because, in general, the purpose is to identify where issues are and how to set priorities for improvements. The purpose is not to assess the level of adherence to the control objectives."

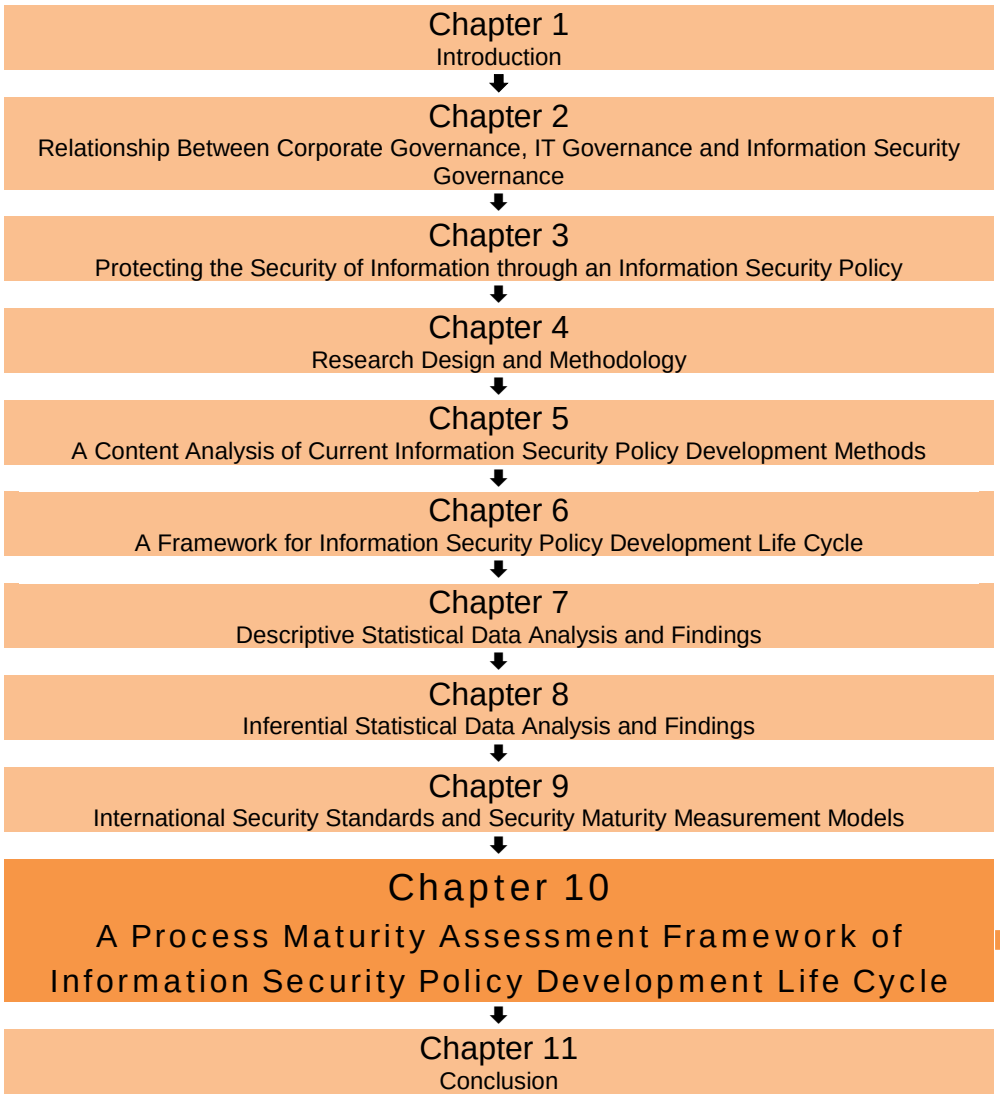
The above assertion provides evidence that COBIT follows a continuous approach while ISO/IEC uses a staged maturity assessment. This will be further discussed in Chapter 10 in the framework implementation section. Table 9.4 depicted the COBIT 4.1 and ISO/IEC 21827 maturity levels requirements and the maturity requirements of the two models.

9.5 Conclusion

The use of maturity models helps an organisation to assess its processes and, thereby, promote process improvement. This research project explores current maturity models and their benefits in terms of evaluating an organisation's information security management. In view of the nature of this research project which is oriented towards an organisation's information security, the two well known international standards, COBIT and ISO/IEC 21827, were chosen as the standards that an organisation should consider in assessing the maturity its information security policy development and implementation processes. COBIT's main focus in on the governance of IT functions, while ISO/IEC 21827 concentrates on the application development processes. A comparison between the maturity levels of COBIT and SSE-CMM was conducted. The findings revealed that a synergy between the two security maturity models.

In Chapter 10 a process maturity assessment framework for the information security policy development life cycle is proposed, based on the maturity criteria that were identified in this chapter.

Chapter 10: A Process Maturity Assessment Framework of Information Security Policy Development Life Cycle



CHAPTER 10:

A Process Maturity Assessment Framework of Information Security Policy Development Life Cycle

10.1 Introduction

The saying that "*if you can't measure it, you can't manage it*" (Browne, 1997) is perhaps one of the most important statements that the information security policy development team should consider during an information security policy development and implementation process. Chapter 9 investigated the current available international standards and security maturity measurement models and their role in assessing the processes of security quality assurance. The mapping between the COBIT 4.1 and ISO/IEC 21827 maturity levels revealed a number of maturity criteria that should be considered before the claim is made that a certain maturity level has been attained.

The main objective of this chapter is to propose a process maturity assessment framework for the information security policy development life cycle and which is inspired by the ISO/IEC 21827 and COBIT 4.1 maturity models. The proposed framework will enable climbing the "ladder" of the information security policy development life cycle using a capability maturity model approach. ISO/IEC 21827 (2008) highlights that it is essential that an organisation perform certain base practices of the process areas as part of an engineering process in order to claim that it has reached a certain maturity level. It is, thus, important to integrate the process areas and maturity levels.

10.1.1 Integrating maturity levels and process areas

The study conducted by Petch, Calverley, Dexter, and Cappelli (2007) showed the relationship between process areas, base practices, phases and capability maturity levels. This study adapted Petch et al.'s (2007) e-Learning Maturity Model (eMM) because the model contains a comprehensive discussion on the integration of maturity levels and processes. Petch et al.'s (2007) study focused on piloting a process maturity model as an e-learning benchmarking method. Their proposed model discusses the components of an e-Learning Maturity Model (eMM) and the relationship between these components. Figure 10.1 depicts the relationship between the eMM components diagrammatically.

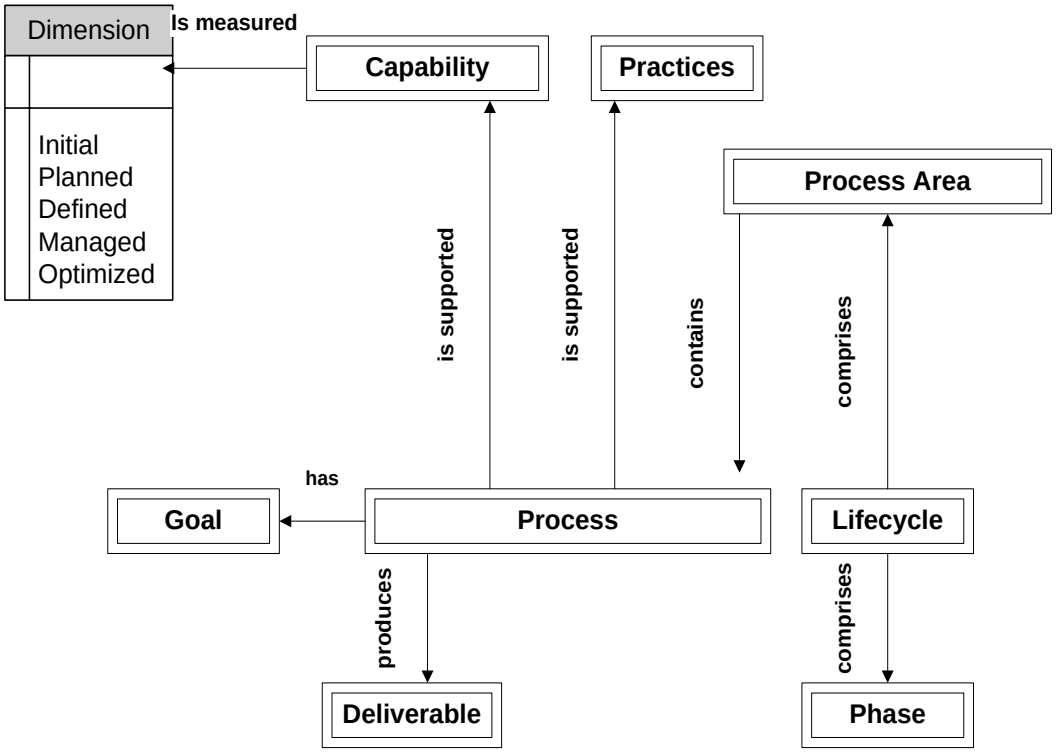


Figure 10.1: Conceptual Model of the eMM and its links to the e- Learning Lifecycle (Petch et al., 2007)

Figure 10.1 shows that a **life cycle** of e-learning encompasses phases which comprise **process areas**. The process areas, in turn, encompass **processes**. Petch et al. (2007, p. 15) defined a process in the eMM as "a description of the goal of a set of activities, each of which will be the responsibility of some role(s) and carry constraints concerning the timing and manner of their execution". A set of activities or processes must be accomplished for an organisation to claim that it has reached a certain maturity level.

Based on knowledge gained in Figure 10.1, we deduce the relationship between components that constitute the proposed framework for this study. An information security policy development life cycle comprises of phases and process areas. The process areas are constituted of processes which are assessed by maturity levels. Figure 10.2 illustrates the relationship between the mentioned components.

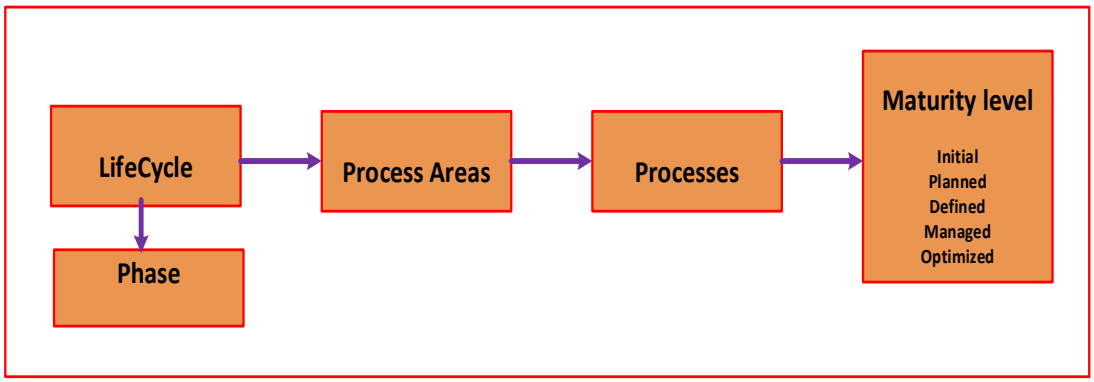


Figure 10.2: Relationships between lifecycle, process areas, processes and capability maturity levels (ISO/IEC 21827, 2008)

Table 10.1 proposes an integration of COBIT, ISO/IEC 21827 process areas, processes and maturity requirements with the information security policy development life cycle processes.

Table 10.1: Relationship between COBIT, ISO/IEC 21827 process areas, processes, maturity levels and ISPLC processes

Maturity level	COBIT 4.1	ISO/IEC 21827	Maturity requirements	ISO/IEC 21827 Process Areas	ISPDLC Phases	Security policy processes
Level 0	Non-existent					No process required
Level 1	Initial	Performed informally	• Risk identified • Need to protect organisation's information • Base practices performed	• PA 02 Assess Impact • PA 03 Assess Security Risk • PA 04 Assess Threat. • PA 05 Assess Vulnerability	Risk assessment	• Assets identification • Vulnerability and threats assessment • Risk identification • Legislation • Risk appetite • Evaluating existing security measures • Risk assessment documentation
Level 2	Repeatable but intuitive	Planned and tracked	• Controls identified • Process planned and managed • Controls operation depend on individuals knowledge	• PA 09 Provide Security Input • PA 10 Specify Security Needs	Information security policy construction	• Write high level security policy • Write detailed security policy • Write lower level security policy • Stakeholders' consultation
Level 3	Defined	Well defined	• Employees awareness • Process implementation • Process well defined • Controls are documented	• PA 07 Coordinate Security	Information security policy implementation	• Security policy awareness • Security policy training • Stakeholders' role • Security policy education
Level 4	Managed and measurable	Quantitatively managed	• Process evaluation • Processes are automated • Processes are reviewed	• PA 01 Administer Security • PA 08 Monitor Security Posture	Information security policy monitoring and compliance	• Non periodic review • Automated review • Review the audit information • Periodic review • Existing theories
Level 5	Optimized	Continuously improving	• Process improvement • Control evaluation • Defects analysed	• PA 11 Verify and Validate Security • PA 06 Build Assurance Argument	Information security policy assessment	

Each of the five maturity level is discussed in the section below:

10.1.1.1 Maturity Level 0: Non - existent

At this level there is a complete lack of any processes in the organisation (COBIT, 2007). Management does not consider security of information as a priority of its business strategy and, thus, management does not assess the business threats and risks.

10.1.1.2 Maturity Level 1: Initial

At **maturity level 1**, the organisation has recognised the need to protect its information from both internal and external threats (ISO/IEC 21827, 2008). The organisation is conscious of the possible consequences should the organisation not implement security protection mechanisms. The organisation is, therefore, ready to embark on assessing risk. This phase is known as known as **Risk assessment**. The risk assessment phase identifies the business assets which an organisation wants to protect, and identifies potential threats to such assets.

The four process areas (PA02: Assess impact, PA03: Assess security risk, PA04: Assess threat and PA05: Assess vulnerability) must be accomplished if a risk assessment plan is to be formulated (ISO/IEC 21827, 2008). As discussed in Chapter 8, the following processes of risk assessment must be conducted: assets identification; vulnerability and threat assessment; risk identification; legislation identification; risk appetite; evaluating existing security measures, and risk assessment documentation. The result of the risk assessment plan will be used to decide what to incorporate into the security policies in order to ensure that the risks which have identified are mitigated.

Table 10.2 depicts the phase, process area and processes that an organisation must implement in order to claim that it has reached maturity level 1.

Table 10.2: Maturity level 1 requirements

Maturity level	Maturity requirement	Phase	Process Area	Processes
Maturity level 1	• Risk identified • Need to protect organisation's information • Base practices performed	Risk assessment	• PA02 Assess Impact • PA03 Assess Security Risk • PA04 Assess Threat • PA05 Assess Vulnerability	• Assets identification • Vulnerability and threats assessment • Risk identification • Legislation • Risk appetite • Evaluation of existing security measures • Risk assessment documentation

The following section discusses the maturity level 2 requirements.

10.1.1.3 Maturity Level 2: Repeatable

Maturity level 2 is characterised by processes that are repeatable, managed and planned (ISO/IEC, 2008). COBIT (2007) states that performance depends on individual knowledge and effort and, thus, in this case the security policy development team members must to use their knowledge to assess the risk and threats that an organisation faces. ISO/IEC 21827 (2008) requires controls to be identified at this maturity level. In this case, a security policy would be the main control that the organisation would implement in order to mitigate the risks identified during the risk assessment stage.

The two process areas, namely, PA09: Provide security input and PA10: Specify security needs, are part of this stage because they are aimed at building a solution, in this case, developing the security policy. During this phase, it is essential that the various stakeholders agree on the security requirements needed in order to mitigate the risks identified during the risk assessment phase. The information acquired during and produced by this process area is collected, further refined, used, and updated throughout the project (PA09: Provide security input) in order to ensure that the needs of the organisation stakeholders are addressed. Next, management must evaluate the costs and benefits of implementing the recommended controls to reduce risk to an acceptable level. If the envisaged expense is within the budget, the next step of policy construction may commence.

As discussed in Chapter 8, the following processes of information security policy construction must be executed, namely, write high level security policy; write detailed security policy; write lower level security policy, and consultation with stakeholders. Table 10.3 shows the phase, process area and processes that an organisation must implement to claim that it has reached maturity level 2.

Table 10.3: Maturity level 2 requirements

Maturity level	Maturity requirement	Phase	Process Area	Processes
Maturity level 2	• Controls identified • Process planned and managed • Operation controls depend on individuals knowledge	Information security policy construction	• PA09. Provide Security Input • PA10. Specify Security Needs	• Write high level security policy • Write detailed security policy • Write lower level security policy • Consultation of stakeholders

The next section discusses the maturity level 3 requirements.

10.1.1.4 Maturity Level 3: Defined

Maturity level 3 is characterised by well defined processes (ISO/IEC 21827). COBIT (2007) states that processes have been standardised, documented, and communicated through training. This phase involves implementing the solution, in this case, the implementation of the security policy throughout the organisation. This, in turn, requires a mechanism in terms of which to communicate with, train and educate the various stakeholders as regards the new information security policy. The process area PA07: Coordinate security ensures that all parties are aware of and involved with security.

The following processes of information security implementation must be executed, namely, information security policy awareness; information security policy training; information security policy education and the role of stakeholders. At this stage, the organisation may be said to be at Maturity level 3 (Well defined) because an information security policy is in place and has been communicated to all the various stakeholders. Next, it is important to monitor the security policy in order to ensure both its enforcement and compliance with the policy. Table 10.4 shows the phase, process area and processes that an organisation must implement to claim that it has reached the maturity level 3.

Table 10.4: Maturity level 3 requirements

Maturity level	Maturity requirements	Phase	Process Area	Processes
Maturity level 3	• Employee awareness • Process implementation • Process well defined • Controls are documented	Information security policy implementation	PA07 Coordinate Security	• Information security policy awareness • Information security policy training • Role of stakeholders • Information security policy education

The next section discusses the maturity level 4 requirements.

10.1.1.5 Maturity Level 4: Managed and measurable

Maturity level 4 is characterised by processes that are both managed and measurable (COBIT (2007). COBIT (2007) recommends that management monitors and measures compliance with procedures and takes action where processes appear not to be working effectively. According to ISO/IEC 21827, the main difference between maturity level 3 and maturity level 4 is that, at maturity level 3, processes must be well defined while maturity level 4 requires the processes to be quantitatively understood and controlled. ISO/IEC 21827 highlights that the processes are quantitatively analysed in order to ensure that their capabilities are understood and to enable their performance to be predicted, thereby improving the organisation's maturity level.

This phase involves the information security policy monitoring and compliance. Accordingly, the two process areas: PA01: Administer security control and PA08: Monitor security posture, need to take place. The objective of PA01: Administer security control is to ensure that the intended security is achieved in its operational state while PA08: Monitor security posture concentrates on ensuring that all breaches of security are identified and reported (ISO/IEC, 21827). The following processes should be executed in respect of the information security policy monitoring: non periodic review, automated review, review of audit information and periodic review. In addition, it is necessary to check the information security policy compliance mechanisms. This may be achieved by understanding the employees' behavioural intention as regards either complying with or violating the policy. It is essential that management understand, for example, existing theories related to information security policy compliance such as the TBP and GDT. Table 10.5 depicts the phase, process area and processes that an organisation must implement to claim that it has reached the maturity level 4.

Table 10.5: Maturity level 4 requirements

Maturity level	Maturity requirements	Phase	Process Area	Processes
Maturity level 4	• Process evaluation • Processes are automated • Process are reviewed	Information security policy monitoring and compliance	• PA01 Administer Security • PA08 Monitor Security Posture	• Non periodic review • Automated review • Review of audit information • Periodic review • Existing theories: o TPB o GDT

The following section discusses the maturity level 5 requirements.

10.1.1.6 Maturity Level 5: optimised

Maturity level 5 is the highest maturity level and is characterised by processes that are optimised. The quantitative performance goals or targets which were identified in maturity level 4 are used to establish the effectiveness and efficiency of the process (ISO/IEC 21827, 2008). COBIT (2007) highlights that processes have been refined to a level of good practice based on the results of continuous improvement and maturity modelling with other enterprises.

This phase encompasses two process areas: PA 06: Build assurance argument and PA 11: Verify and validate security. The objective of PA 11: Verify and validate security is to ensure that solutions are verified and validated with respect to security; while PA 06: Build assurance argument focuses on conveying that the information that the customer's security needs have been are met (ISO/IEC 21827, 2008).

For an organisation to be at maturity level 5 (Optimised) the requirements of the security policy which has been implemented must meet the customer's security requirements. The data gathered in maturity level 4 is analysed to ascertain the causes of any defects with the objective of preventing known types of defects from recurring (Lutteroth et al., 2007).

At this stage, organisations must have effective assessment strategies in place. As discussed in Chapter 8, assessment must be conducted throughout the whole information security development life cycle. At maturity level 5, the life cycle needs to be repeated

from Phase 1: Risk assessment. There are numerous unknowns during the last phase and an organisation may identify a new threat that was not considered, a new regulation requirement that is needed, or a business capability that was forgotten and which must be catered for in the organisational policies. The process of assessing the information security development life cycle is important because this helps to identify flaws and defects that were not foreseen in the initial development process. Accordingly, this study recommends that assessment take place throughout the information security policy development life cycle. This is illustrated in the proposed maturity assessment below by the arrows going backwards between the different phases of the cycle. Through a reiterative process, the organisation constantly improves its capability and deploys rapid changes in order to manage its processes. Table 10.6 presents the phase, process area and processes that an organisation must to implement to claim that it has reached the maturity level 5.

Table 10.6: Maturity level 5 requirements

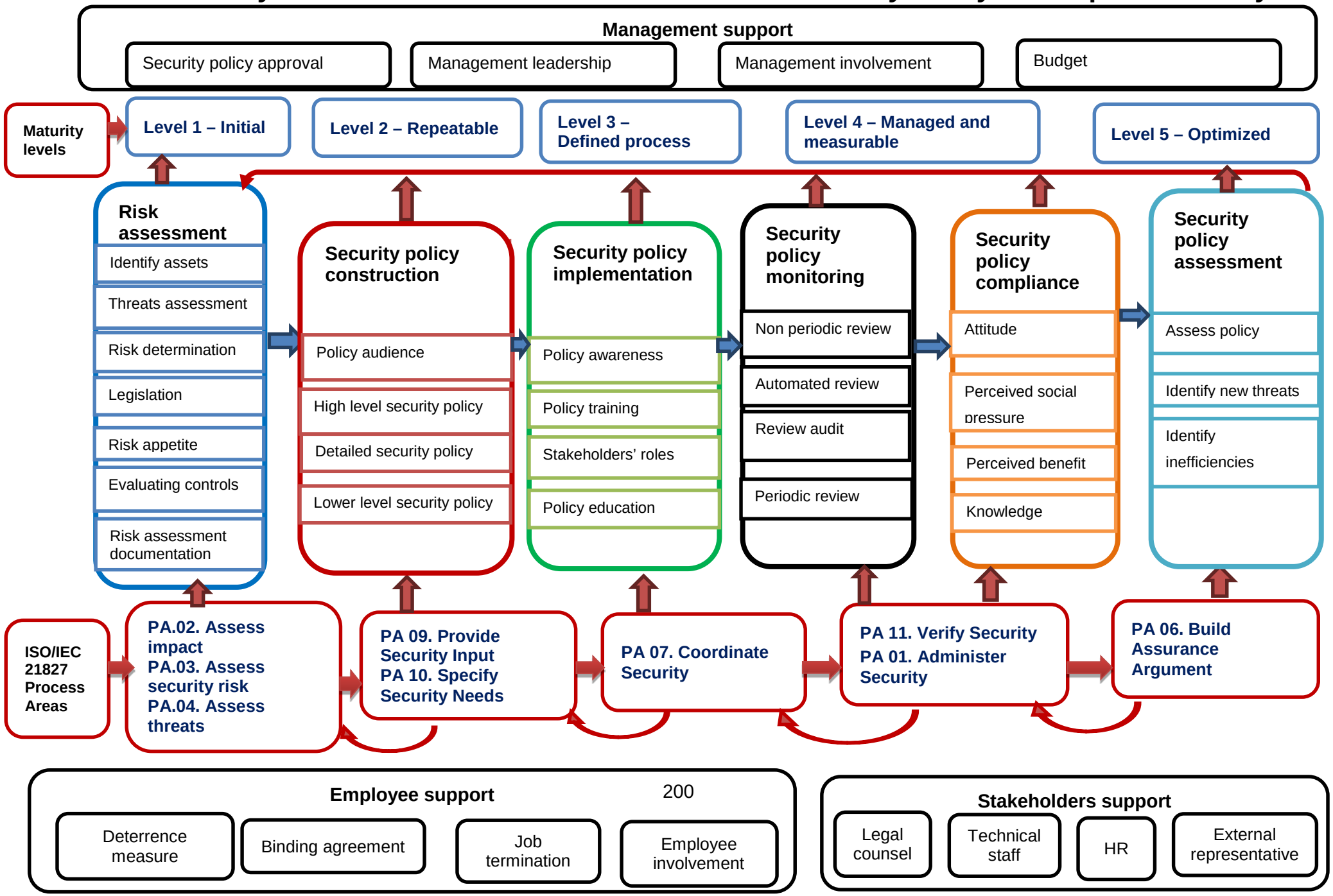
Maturity level	Maturity requirements	Phase	Process Area	Policy processes
Maturity level 5	• Assure the customers security needs have been met • Analyse the defects • Identify the inefficiencies • Improve processes	Information security policy assessment	• PA 11 Verify and Validate Security • PA 06 Build Assurance Argument	• Security policy assessment • Identify inefficiencies • Identify new threats

Based on the knowledge gained from the discussion of the integration of the process areas and maturity levels, a maturity framework assessment for the information security policy development life cycle is proposed in the next section.

10.2 A process maturity assessment framework for the information security policy development life cycle

The proposed framework incorporates the maturity assessment dimension in the framework that was proposed in Chapter 6. The proposed maturity assessment framework is shown below.

A Process Maturity Assessment Framework of Information Security Policy Development Life Cycle



The proposed maturity assessment framework will enable an organisation to focus on the process areas and processes of the information security policy development life cycle in order to reach a specific maturity level. The ideal target would be to reach the highest maturity level 5. The proposed maturity assessment will enable an organisation to determine the processes which are needed to improve the maturity level and, therefore, build a defined, measurable and optimised process of developing and implementing information security policies.

10.2.1 Implementation of the framework: staged versus continuous maturity assessment

Ferraiolo and Sachs (2000) differentiate between continuous and staged maturity models. They argue that, in a staged model, the organisation must implement a specific process area at a given stage. However, in a continuous model, maturity is not as clearly defined for a specific application but, rather, process areas are used to organise the practices for the specific application as opposed to defining the maturity at a specific level. The framework proposed in this study is a guide that organisations should follow in order to assess their information security policies, and, thus, the implementation of the proposed processes should follow a continuous approach.

On the other hand, the maturity assessment should follow the staged approach. Undoubtedly, certain institutional aspects would need to be in place before others may be effective. For example, it is not possible for processes to be effectively measured or quantitatively controlled (Level 4) until they have been well defined (Level 3). Being qualified at level n means the current information security policy has satisfied, to an acceptable degree, all the security requirements of both level n and the lower levels. In other words, lower level security requirements should be satisfied first, at least to a reasonable extent, before moving to the next level.

The proposed framework evaluates the processes of the information security policy development life cycle on five maturity level scales. Maturity level one and maturity level five are the lowest and the highest maturity levels respectively. In addition, the framework suggests that maturity assessment should take place throughout the entire process of the information security policy development life cycle.

10.2.2 Benefits of the proposed maturity assessment framework

By using the proposed maturity assessment framework, organisations will gain the following benefits:

- Assist organisations in maturing their security level to improve the business operations and business continuity, which are affected by processes.
- Organisations will be able to better understand, define, control, and improve their processes of developing and implementing information security policies.
- The framework acts as a check of strengths and weaknesses judged against the key maturity requirements specified in the framework.
- Enable organisations to compare their maturity levels with those of other organisations with similar portfolios.
- Enable organisations to identify what levels have attained high maturity and those that are lagging behind and require more attention; and
- Enable organisations to identify the key process areas and process that are required to achieve a specific maturity level.

The next section discusses the evaluation of the framework by security experts.

10.3 Framework evaluation based on the expert review

This section discusses the findings of the experts who critically reviewed the proposed framework. A total of seven experts in the information security field were approached and requested to critically analyse the main contribution of this study, namely, the framework depicted in Figure 10.2.1. The experts are academically recognised because they have published extensively in the information security field. Simon (2011) maintains that it is crucial to provide experts with guides or instruments to ensure that different aspects of a study are reviewed critically. In this study, each expert was provided with a hard copy of the framework and the research methodology diagrams. In addition, the researcher delivered a presentation to the experts to ensure that they understood the study under review.

The proposed maturity assessment framework is based on the content analysis of existing information security policy development and implementation methods. In order to

ensure research rigour, the content analysis research technique followed Krippendorff's (2004) six steps for conducting a content analysis. During the selection of the sample, different criteria were used such as the reputation of the author which depended, for example, on the number of people who had cited the article, while the reputation of the journal or the conference of the paper was also considered. In addition, the study relied on well-known theories such as the TPB and GDT.

The proposed framework was evaluated based on the evaluation criteria recommended by Webber (2012). Webber (2012) discusses criteria that should be used in the evaluation of theories in the information systems discipline.

10.3.1 Importance

Corley and Gioia (2011, p. 17) state that "the importance (or utility) of a theory is often assessed via judgments made about the importance of its focal phenomena." Webber (2012) points out that there is little point in having a theory with rigorously specified constructs if the theory addresses uninteresting phenomena.

The experts were asked questions in order to ascertain their opinions about the importance of the proposed framework:

Question: *Does the framework address a relevant problem or future problem?*

The seven experts all agreed on the importance of the proposed framework. One expert stated: "Yes, the framework addresses the relevant issue. I like the fact that you address risk assessment at the beginning of the framework. One of the drivers of security policy development is risk management, which is the whole reason for the existence of security policies."

10.3.2 Novelty

Colquitt and Zapata-Phelan (2007) and Corley and Gioia (2011) state that "the extent to which a theory is novel is an important factor determining (a) the value ascribed to it by researchers, and (b) the likelihood that papers describing the theory will be accepted for publication in major journals."

The experts were asked the following question in order to ascertain their opinions about the novelty of the framework:

Question: *Does the framework provide novelty? Have you found any similar framework or theory with similar structure and concepts?*

The seven experts all agreed that the framework was novel. They stated the following:

- "The framework proposed is a good contribution to the information security field. I commend your attempts to bring some quantitative evaluation to a subject which is poorly understood."
- "The framework proposed provides a very relevant issue. Mostly, security policies are developed without much thought of rigour".

10.3.3 Constructs

According to Webber (2012), "a construct in a theory represents an attribute in general of some class of things in its domain (as opposed to a particular attribute of a specific thing)". The experts were asked the following question in order to find out their thoughts on the constructs of the framework:

Question: *Based on the proposed framework, do you think the constructs provided are important to the security policy development team who are responsible of developing and implementing security policies? Please suggest any additional construct that you deem important or remove the ones that you feel are not important.*

The feedback comments and how the feedback was addressed are presented in Table 10.7.

Table 10.7: Expert feedback on framework constructs

Expert feedback	How the feedback was addressed?
"In the security policy guidance box, you need to add guidelines as well, in addition to international standards."	This was addressed by adding guidelines as a new security policy guidance factor.
"Under risk assessment, there is a need to know past risk situation. Knowing risk is one thing, but knowing how many security breaches the company had before is relevant."	This recommendation was addressed by the risk assessment documentation process.

10.3.4 Parsimony

Webber (2012, p. 15) states that "parsimony theories achieve good levels of predictive and explanatory power in relation to their focal phenomena using a small number of constructs and associations". Miller (1956) recommends that a small number of constructs should be equal to "number seven, plus or minus two". In view of the nature of

this study, this criterion was not met because the main objective of this study was to explore all the possible processes that an information security policy goes through its life time. Accordingly, the study focused on more than seven processes.

10.3.5 Level

Webber (2012) argues that there are two types of theories, namely, micro-level and macro-level. Webber (2012, p. 15) points out that "micro-level cover a very narrow, constrained set of phenomena; while a macro-level theory might be compelling because it provides broad, overall insights into many phenomena." The proposed framework is a micro-level theory because it covers a specific area only, namely, the maturity assessment of the information security policy development life cycle. In addition to the evaluation criteria proposed by Webber (2012), the experts were given an opportunity to give their opinions or offer suggestions that may improve the framework.

10.3.6 Suggestions for the improvement of the framework

The experts were asked to provide input for improvement of the framework.

Question: *Please suggest any ideas that may improve the framework.*

Table 10.8: Expert suggestions for improvement of the framework

Expert feedback	How the feedback was addressed
"There is a need to have a feedback loop to cater for changes in case some processes have been left out and later needed to be added. For example, you are on phase 2 of security policy construction and you noticed that some changes need to be done in phase 1 of risk assessment. Every change cannot be described as static".	This recommendation was addressed in the framework by drawing arrows that illustrates the iterative feedback between the constructs.
"It could be interesting if you can indicate clearly how management and employee support are linked to the other constructs".	This comment was addressed in Chapter 10 which discussed the relationship between management and the ISPDLC constructs. The chapter also explored the employee support and ISPDLC constructs.
"It is important that you indicate that compliance and monitoring are recursive never-ending activities – even if the information security policy itself doesn't change."	This comment was addressed in the framework construction by adding arrows that show iterative design.

Expert feedback	How the feedback was addressed
"Users in the organisation need to be consulted during the process of developing security policy so that they accept the new policy during the implementation stage".	This comment was addressed in the framework construction under the employee involvement factor. The involvement of the employees in the entire process of developing information security policy will increase.
"In the framework, there are arrows between different constructs. Arrows represent relationship. The characteristics of relationship must be described".	This comment was addressed in Chapter 8. In Chapter 8, statistical tests were conducted to ascertain whether there is a relationship between the various constructs of the proposed framework. The findings revealed that there is a positive correlation between the different constructs and, thus, provide proof of the existence of the relationship.

The experts were also asked to give their opinions on the research methodology used.

10.3.7 Research methodology used

The experts were asked to provide feedback on the research methodology used in the study.

Question: *Do you think the research methodology used was appropriate for this research project?*

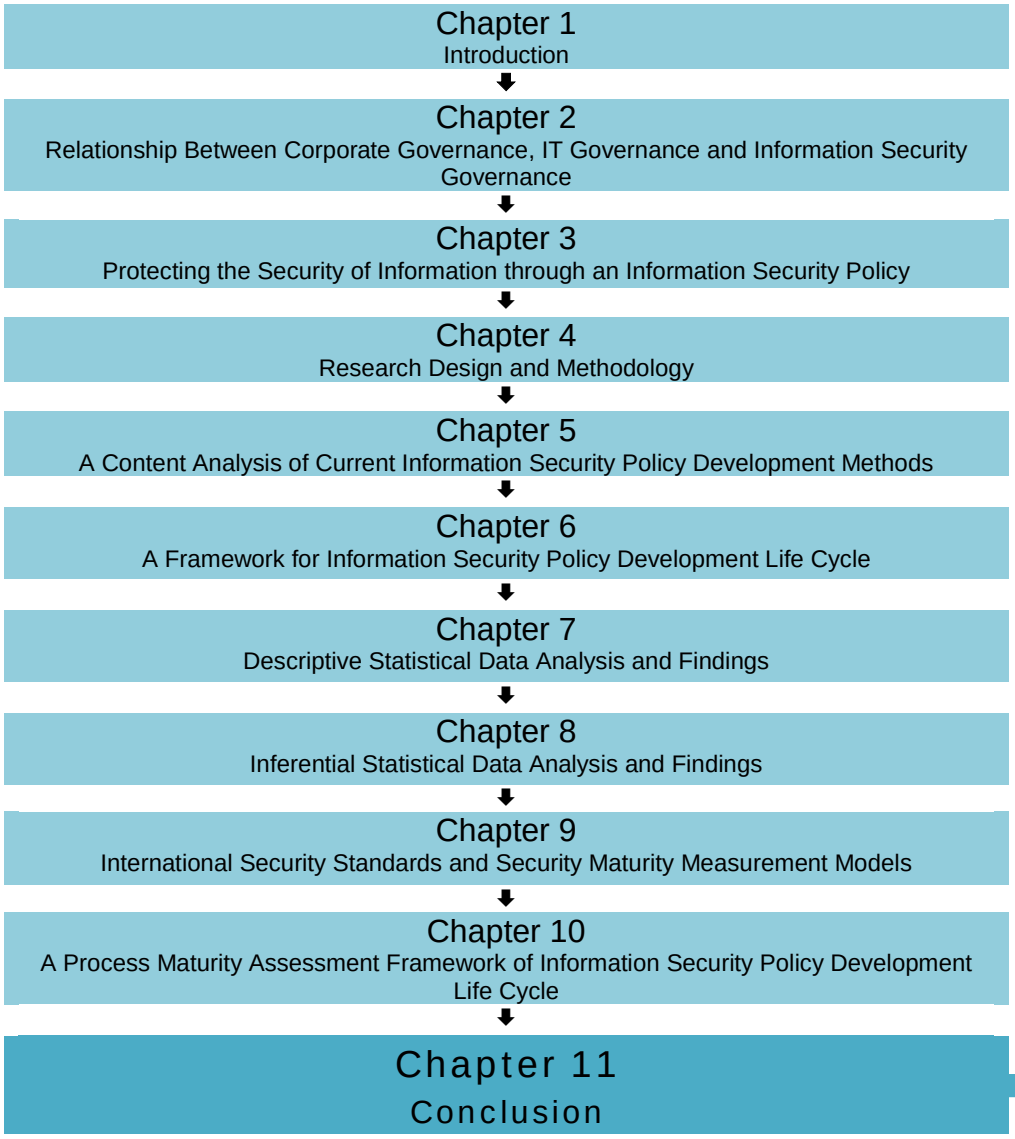
The seven experts all agreed that the appropriate research methodology had been used. Below is some of the feedback provided:

- "Yes, the methodology used is appropriate. I like the fact that sampling of the documents of the content analysis contained industry publications which entailed that practitioners' input are taken into account."
- "Yes, I agree on the methodology used. Mixed method is important because it increases the validity of research findings. The strengths of one research approach can compensate for the weaknesses of the other approach."
- "Design science is increasingly used as a research methodology in designing and evaluating IS models and frameworks. I am happy you have used this research methodology."

10.4 Conclusion

Based on the ISO/IEC 21827 and COBIT 4.1 process maturity levels, the chapter proposed a framework for the assessment of the processes of information security policy development and implementation. The framework presents an integrated and holistic approach to ensuring the incremental process maturity of an organisation's security stance and the performance of the security policy development process. The framework provides an evolutionary path from an ad hoc information security policy development approach to a more structured, defined, manageable and repeatable quality approach that protects the critical information of an organisation and allows for milestones to be created, measured and met in a projected manner. In addition, organisations using the proposed framework will be able to determine the current maturity levels of their information security policy development process and be able to plan enhancements in the correct order. The next Chapter will conclude this research project.

Chapter 11: Conclusion



CHAPTER 11:

Conclusion

11.1 Overview

Threats to corporate information are constantly increasing at a time when businesses are relying more heavily upon information technology than before. Accordingly, it has become evident that security managers must have proper controls in place to ensure the security of the organisation's information. This, in turn, entails an appropriate and effective information security management plan. This study states that an effective information security policy is the main security control which may be used to protect an organisation's information assets.

This chapter summarises the overall research project by focusing on the achievements and findings of the study. The framework presented in the study was based on secondary data collected from a review of existing literature on information security policy development and implementation methods. The primary data which was used to validate the proposed framework was collected by means of a survey. In addition, the feedback suggestions of the respondents to the survey were used to refine the framework. The framework was then further refined through an expert review process. This chapter highlights how the research objectives were met in order to answer the research questions posed by the study. The chapter discusses the theoretical framework; the research methodology used; research evaluation and, finally, the limitations of study. Finally, the chapter offers recommendations for future research.

11.2 Research project contribution

The main contribution made by this study is the development of a process maturity assessment framework of the information security policy development life cycle. This framework is intended to serve as a guide to information security practitioners in the process of developing and implementing information security policies. The proposed framework indicates the various steps needed in the development, implementation and enforcement of an effective information security policy. In addition, the study emphasises the importance of integrating security maturity assessment into the information security policy development life cycle. Furthermore, the framework offers a structured methodology for evaluating the maturity level of an information security policy and offers a roadmap for the ongoing progression and improvement of the processes of developing and implementing information security policies. The following section discusses the research objectives of the study.

11.3 Research objectives

The main objective of this study was to provide a framework which would ensure a comprehensive structured methodology for assessing the maturity level of an information security policy. In addition, such a framework offers a roadmap for the information security policy development life cycle which promotes sustainability.

In order to realise the main research objective mentioned above, the following secondary objectives were addressed:

1. **Discuss the importance of implementing effective information security policies and then introduce such policies as important facets of Information Security Governance.**

   Chapter 2 discussed the relationship that exists between Corporate Governance, IT Governance and Information Security Governance. Chapter 2 emphasised that it is incumbent on the executive management of an organisation to be both committed to and responsible for information security because this is required by law while it also promotes good Corporate Governance within the organisation. It is, thus, evident that executive managers must put in place proper controls to ensure the security of the organisation's information as this will result in an appropriate and effective governance structure. In order to realise this objective, the research project emphasised the important role of proper information security policies in effective Information Security Governance. The chapter argued that an information security policy development, which comprises well-planned processes of security policy construction, implementation and enforcement, is vital to ensuring the information security of an organisation.

2. **Determine the major processes required in developing, implementing and adopting effective information security policies.**

   This research objective was addressed in Chapters 5 and 6. Chapter 5 described the content analysis of current information security policy development methods that was conducted using secondary sources in order to obtain a deep understanding of the processes that are critical for the information security policy development life cycle. The findings of the content analysis revealed seven categories that are considered to be the main pillars of the information security

policy development life cycle. In Chapter 6, the seven categories that had emerged in Chapter 5 were analysed and interpreted so that a solution for to research question posed in the research project could be inferred from the categories. The main objective of Chapter 6 was to discuss these seven categories in depth. Based on the categories, a conceptual framework was developed. The framework was then refined in two stages. In the first stage, the framework was refined based on the feedback suggestions of security professionals who had participated in the survey while, in the second stage, the framework was refined based on feedback from the expert reviewers. A refined framework was then produced.

3. **Investigate the importance of information security policy development life cycle processes from the view point of security professionals.**

Chapter 7 presents the descriptive statistical data analysis and findings that resulted from the primary data that had been collected from the survey. The main objective of the survey was to assess the importance of the conceptual framework constructs which had emerged in Chapter 6. Each of the seven constructs includes four processes. The respondents were asked to indicate the importance of both the constructs and their processes.

The findings of the survey revealed that the majority of the respondents (85.53%) had indicated that there was an information security policy in place in their organisations while (14.47%) had stated that their organisations did not have such a policy in place. However, the results clearly showed that the respondents believed that an information security policy is the main security control which may be used to mitigate an organisation's security risks.

The findings also showed that respondents believed that all seven constructs were important. In addition, the results showed that risk assessment was very important as compared to the other constructs of the information security policy development life cycle. Management support was ranked in second place after risk assessment. Risk assessment is an important process as it is essential that an organisation constructs its information security policy based on the result of the risk assessment. In addition, management is in charge of an organisation's daily activities and, thus, management plays a crucial role in the formulation of the information security policy.

4. **Determine whether there is a relationship between the management support, employee support and the information security policy development life cycle.**

Chapter 8 focussed on the investigation of the relationship between the constructs of information security policy development life cycle. These were discussed in terms of 2 categories:

Correlation analysis between management support and the information security policy development life cycle processes

A key assumption made in Chapter 6 in which the framework of this study was proposed was that it is of the utmost importance that management is involved in all the Information Security Policy Development Life Cycle (ISPDLC) processes, namely, risk assessment; information security policy construction; information security policy implementation; information security policy monitoring, and information security policy compliance. Chapter 8 discussed the inferential statistical tests that were conducted in order to ascertain whether there was a relationship between management support and the ISPDLC constructs. The findings showed a positive correlation between management support and the ISPDLC constructs with a statistically significant result.

Correlation analysis between employee support and information security policy development life cycle processes.

In Chapter 6 the assumption was made that there must be employee support as regards all the ISPDLC constructs. Chapter 8 discussed the inferential statistical tests that were conducted in order to ascertain whether there was a relationship between employee support and the ISPDLC constructs. The findings confirmed the existence of a significant relationship between employee support and the ISPDLC constructs.

5. **Investigate existing security maturity measurement models and their role in assessing an organisation's information security management.**

Chapter 9 explored the existing theories and maturity models found in the literature and their benefits in terms of evaluating an organisation's information

security management. This research project used the ISO/IEC 21827 standard and COBIT 4.1 security framework as a guide in the maturity assessment of the information security policy development life cycle. These two security maturity models were chosen because they are recognised internationally. In addition, they are information security based and are widely accepted by both practitioners and academia (Abu-Khadra et al., 2012). A high level comparison between the four domain process areas of COBIT and the twenty two process areas of SSE-CMM confirmed that there is a synergy between the two security maturity models (Ahuja and Goldman, 2009).

6. **Identify key characteristics that are necessary in order to assess the maturity of the information security policy development and implementation processes.**

   Based on by the COBIT 4.1 and ISO/IEC 21827, Chapter 8 discussed how to discover the best approach to use in order to evaluate the maturity of the information security policy development life cycle. A mapping between the COBIT 4.1 and ISO/IEC maturity levels was performed with the aim of ascertaining the key maturity requirements that should be used in evaluating the process of developing and implementing information security policies. A process maturity assessment framework of the information security policy development life cycle was proposed. It is anticipated that the proposed framework will enable organisations to “climb the ladder” of the information security policy development life cycle guided by a capability maturity model approach.

11.4 Theoretical framework

Chapter 3 explored the various challenges that organisations face during the development of an information security policy. These challenges included, for example, the lack of available guidance as regards to developing and implementing an information security policy. It was found that there was a gap in the existing methods cited in the literature. The current methods provide basic processes in terms of developing and implementing information security policies. There are some similarities between the methods with authors agreeing on the same steps while there are also gaps where a particular author may not have mentioned a step that the others considered as important. Accordingly, a content analysis was conducted in order to gather the information on the

various processes involved in the information security policy development and implementation methods/approaches cited in the literature.

This study relied on existing theories related to information security policy compliance in order to understand the behavioural intention of employees as regards either complying with or violating an organisation's information security policy. The Theory of Planned Behaviour and General Deterrence Theory were used. The Theory of Planned Behaviour explains that the intention of an individual to perform a given behaviour is influenced by attitude, subjective norms and perceived behavioural control (Fishbein and Ajzen, 1975). On the other hand, General Deterrence Theory predicts that the increase in the severity of the punishment imposed on those who violate the rules of the organisation reduces certain criminal acts (Blumstein et al., 1978). In addition, the two well-known international documents, COBIT 4.1 and ISO/IEC 21827, were chosen as the standards that an organisation should consider in assessing the maturity of its information security policy development and implementation processes.

11.5 Research methodology

Based on the nature of the problem under investigation and the objectives of the study, this study was conducted in terms of the pragmatism paradigm but with significant input from the design science paradigm. The design science paradigm guided the research methodology and research design used in the study. The research methodology involved the mixed method approach which is supported by the pragmatism paradigm. The following characteristics of the mixed method, exploratory, sequential design helped to address the research question which had been formulated at the beginning of the study:

- ✓ Exploration: The objective of the exploratory design used in this study was to generalise the qualitative findings which had been based on a few individuals from the first phase (content analysis) to the larger sample (400 security professionals) which was used during the second phase. The results of the first qualitative method (content analysis) assisted in informing the second quantitative method (survey).

- ✓ Triangulation during data collection: This strategy involves using more than one method in order to address the same research question. Both a quantitative approach (closed questions) and a qualitative approach (open ended) were used in the survey which was conducted.

- ✓ The framework was constructed based on the information from both the qualitative findings (content analysis) and the quantitative findings (survey).
- ✓ The qualitative findings (content analysis) helped in the development of the survey questionnaire which was used in the quantitative phase.

This research project followed the Design Science paradigm. Design Science involves a rigorous process to design artefacts – in this case the framework for assessing the information security policy development life cycle. The seven guidelines proposed by Hevner et al. (2004) were chosen as the main guidance mechanism to find the solution to the problem addressed in the study and were applied as follows:

Design as an artefact: This study produced a process maturity assessment framework for the information security policy development life cycle.

Problem relevance: The following problem was addressed in the study: Which mechanism should an organisation adopt when assessing the maturity of its information security policy development life cycle?

Design evaluation: The design evaluation was conducted in two phases. In the first phase the framework was evaluated by the security professionals who participated in the survey while, in the second phase, the framework was evaluated by experts in the information security management field.

Research contribution: The contribution of this study is the research maturity assessment framework which offers a structured methodology for evaluating the maturity level of an information security policy.

Research rigour: Research rigour exists because the study relied on proven research techniques such as content analysis, a survey and an expert review.

Design as a search process: A critical review of relevant literature was conducted during the content analysis in order to select the most relevant documents available on information security policy development and implementation methods. In addition, the iterative nature of the search process was ensured through the refinement of the framework using feedback from both the survey respondents and the expert review process.

Communication of research: The researcher has already published two papers: one of which was delivered at an international conference and the second at a local conference.

A third paper was submitted in an international journal and it is under review process. The thesis will be available on the internet via the UFH library.

11.5.1 Triangulation

This research project used the **triangulation** approach in terms of which two main research methods were used to address the research problem. Creswell (2009) maintains that triangulation involves "using different data sources of information by examining evidence from the sources and using it to build a coherent justification for themes". The **qualitative method** used involved the content analysis that was conducted in order to gather information on the processes of developing and implementing an information security policy. The processes discovered were brought together to formulate the dimensions that constitute an effective information security policy development life cycle. A **quantitative method** was used to evaluate the importance of the processes which had emerged from the content analysis through the survey in which security experts participated. In addition, the survey used open ended questions to enable the respondents to offers suggestions regarding the improvement of the framework. Figure 11.1 depicts the data collection process followed in this study.

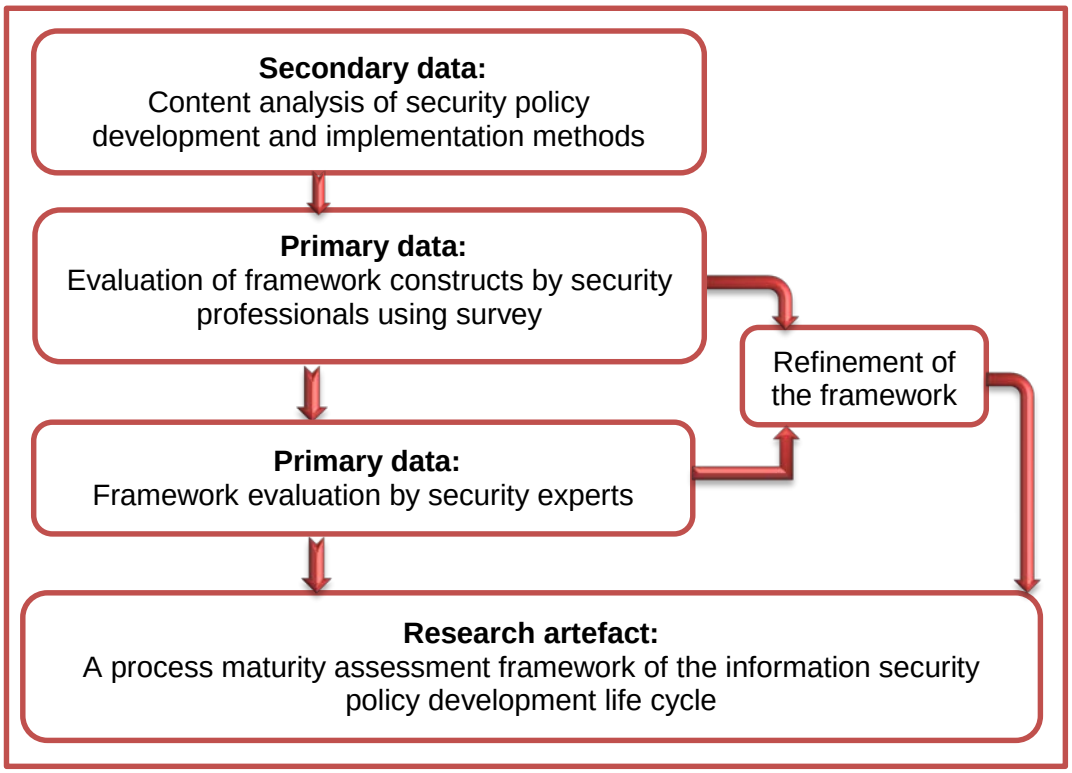


Figure 11.1: Data collection process

The use of mixed methods of data collection allowed the triangulation of the data, thus increasing both the reliability and validity of the study. The next section discusses the research evaluation of the study.

11.6 Research evaluation

In order to ensure both the credibility and integrity of a research project, it is crucial to conduct a research evaluation. This study fulfilled the framework evaluation key criteria as recommended by Van Biljon (2006). These criteria are presented in Table 11.1.

Table 11.1: Framework evaluation key criteria

Framework consideration	Question details	(Van Biljon, 2006)
Verification	Are we building the product right? (Boehm, 1984)	This involves activities to ensure that the framework correctly represents specific concepts.
Validation	Are we building the right product? (Boehm, 1984)	Involves activities that ensure that the proposed framework meets the requirements.
Evaluation criteria	Simplicity, comprehensiveness, Generality and exactness. (Olivier, 2004)	Standard (applicable) criteria.
Usefulness (Utility)	Is the framework able to produce results? (Van Biljon, 2006)	Determining the framework's fitness for a particular use.

Verification

Verification criteria pose the following question: "Are we building the product right?" (Boehm, 1984). This entailed checking that the framework correctly represented specific concepts. In order to meet this criterion, the experts were asked whether they thought the constructs of the proposed framework were important and related to the framework.

Validation

Boehm (1984) states that *validation* is used to check whether the right product has been developed. Cronbach's alpha was used to measure the internal consistency of the questionnaire variables. The findings revealed that the sub-variables asked in the questionnaire in relation to all the combined constructs of the framework were both reliable and consistent. In addition, the questions that were asked in the survey were based on the constructs of the proposed framework.

Evaluation criteria

Olivier (2004) maintains that a framework should meet the following criteria: *simplicity, comprehensiveness, generality* and *exactness* as shown in Table 11.2.

Table 11.2: Evaluation criteria

Criteria	Application to this study
Simplicity	The proposed framework facilitates the understanding of the processes of developing information security policies without additional explanation. The framework is designed for security professionals who should be familiar with the concepts indicated in the framework.
Comprehensiveness	The proposed framework relies on existing information security policy development and implementation information found in the literature.
Generality	The content analysis was conducted on the sample of 21 documents. The results of the content analysis were validated in the survey in which 400 security professionals participated.
Exactness	The framework is composed of nine constructs that comprise the processes that are deemed important for that specific construct. Each construct of the framework may be clearly distinguished from the other constructs.

The following section briefly discusses each of the four criteria.

Usefulness (Utility)

The criterion of usefulness, as cited by Van Biljon (2006), was used to check whether the framework was able to produce results. During the evaluation of the framework experts were asked their opinion of the importance of the proposed framework. All the experts agreed on the importance of the proposed framework. The framework is important because it shows, step-by-step, the processes of developing information security policies.

In addition, Whetten (1998, p. 4) recommends that "any contribution made to theory is to have a descriptive value." They describe a complete theory as comprising four essential elements, namely: What, How, Why and Where. These four elements are discussed below:

What: This element includes the factors, variables, constructs and concepts which are deemed important for the explanation of the phenomenon of interest (Whetten, 1998). The factors that comprised the framework emerged during the content analysis and from the feedback from the security professionals who had participated in the survey as well as

the suggestions of experts. Table 11.3 shows the constructs of the conceptual framework.

Table 11.3: The conceptual framework constructs

Constructs	Factors identified
Risk assessment	Assets identification
	Vulnerability and threats assessment
	Risk identification
	Legislation
	Risk appetite
	Evaluate security measures
	Risk assessment documentation
Information security policy construction	Write high level security policy
	Write detailed security policy
	Write lower level security policy
	Consultation of stakeholders
Information security policy implementation	Information security policy awareness
	Information security policy training
	Role of stakeholders
	Information security policy education
Information security policy monitoring and assessment	Non periodic review
	Automated review
	Review the audit information
	Periodic review
Information security policy compliance	Attitude
	Social pressure
	Benefit of compliance
	Knowledge
Management support	Information security policy approval
	Information security policy enforcement
	Management involvement
	Budget
Employee support	Deterrence measure
	Binding agreement
	Job termination
	Employee involvement
International Standards	Security standards
Information security policy stakeholders	Stakeholders

Funchall (2011) and Whetten (1998) state that the **What** and **How** elements constitute the subject of the theory.

How: “Once a set of factors has been identified, the next question is, How, are they related? Operationally this involves using arrows to connect the boxes” (Funchall, 2011,

p. 87). One of the objectives of this study was to identify the relationship between the processes of the information security policy development life cycle. **Chapter 8** discussed the inferential statistical tests that were conducted to verify these relationships. The results of the tests revealed a positive correlation between the constructs.

Why: Why refers to the reason why the underlying dynamics were selected as factors as well as the proposed causal relationships? (Whetten, 1998). The constructs that comprised the framework were those found in the literature. The factors of the framework became evident through the statistical analysis of the survey conducted in Chapter 7.

Where: The where condition places limitations on the propositions generated from the theoretical model in this study. Once implemented, where would the framework have either an impact or effect? (Funchall, 2011). It is anticipated that, after the proposed framework has been implemented, it will have an impact on the attitudes of employees, management decisions and organisations' processes. Figure 11.2 depicts how these elements were applied to this research project.

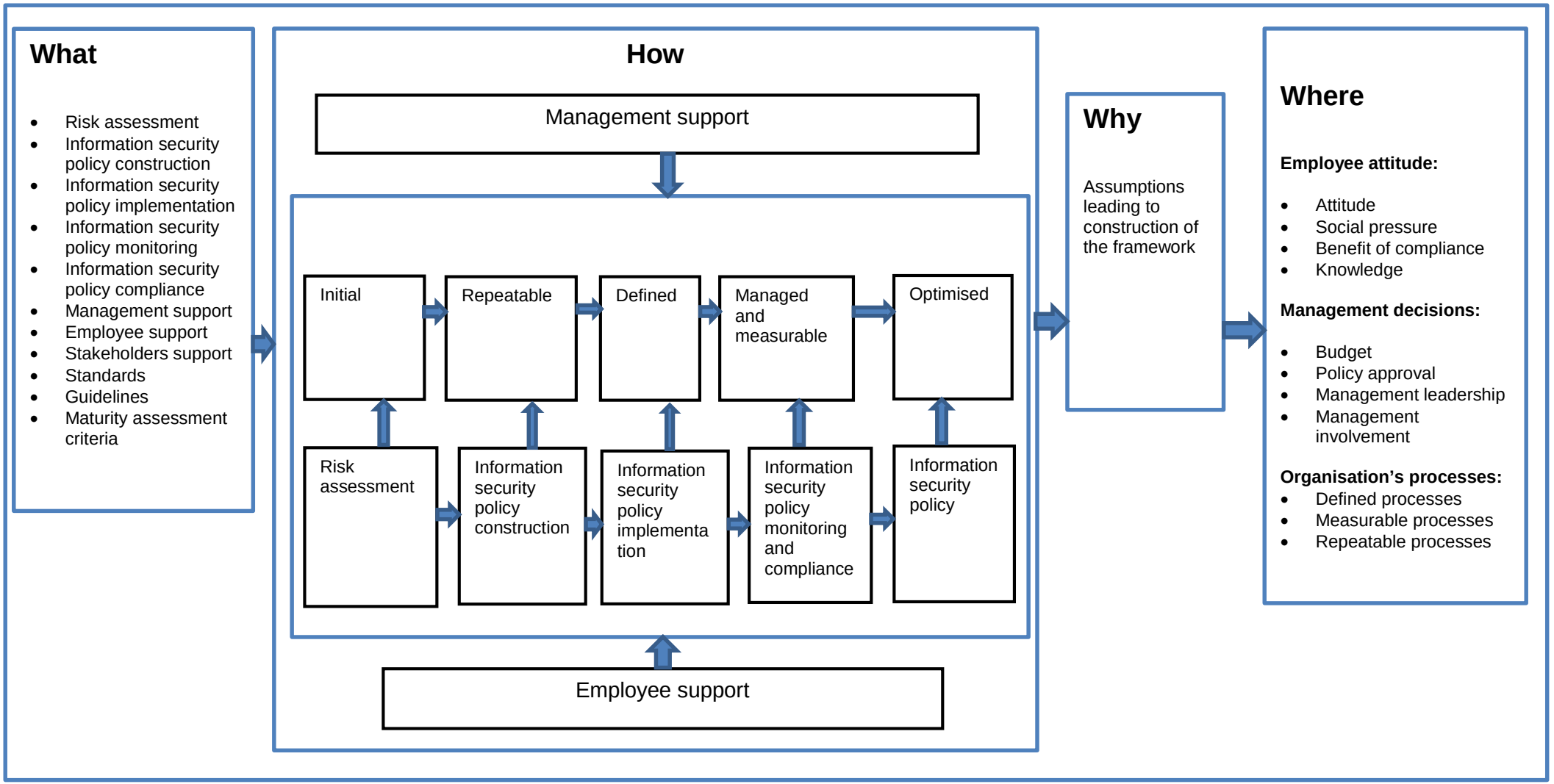


Figure 11.2: Research project evaluation

As depicted in Figure 11.2, these essential elements, defined as *What, How, Why* and *Where*, were applicable to the proposed framework. The next section discusses the key findings of the research project

11.7 Findings of research project

This section briefly highlights the findings of the content analysis, descriptive data analysis and inferential statistics.

11.7.1 Content analysis findings

After ranking papers, the 21 most cited documents that were coded using MAXQDA software revealed 29 codes and 628 accumulative tags. The reducing stages uncovered seven categories that constitute the main pillars of information security policy development and implementation process. These categories are: information security policy construction; management support; employee support; information security policy compliance; information security policy implementation; risk assessment; information security policy monitoring and assessment. The content analysis revealed a high frequency of tags in respect of information security policy construction, management support and employee support, thus implying that they are considered to be important steps that should be in place during an information security policy development and implementation process. The findings also revealed that information security policy monitoring and assessment and risk assessment had the least number of tags.

Based on the results of the content analysis, a conceptual framework of the information security development life cycle was proposed. The proposed framework was refined based on the suggestions of professionals gathered during the survey and further by the expert review feedback. The refined framework comprises five dimensions that constitute the main pillars of the information security policy development and implementation process. These dimensions are: information security policy development life; information security policy drivers; information security policy guidance; people support and existing theories.

The first dimension is the **information security policy development life cycle**. This dimension encompasses the processes required in the development of an information security policy, namely, risk assessment; information security policy construction; information security policy implementation; information security policy compliance, and information security policy monitoring and review.

The second dimension – the **security policy drivers** – is composed of the threats that place the organisation under pressure to institute mechanisms to protect its information. Abdel-Aziz (2010) states that "before discussing information security policy and the process to assess it, it is important to know what drives information security in the first place". The development of information security policy is driven by both external and internal factors that place the organisation under pressure to have in place mechanisms to protect its information. These factors include internal threats such as insider employees who place the organisation's information at risk, as well as external threats such as hackers, crackers, virus and so forth, while, more importantly, there is also the need to comply with the increasing government legislator requirements.

The third dimension – the **security policy guidance** – comprises the security standards that guide organisations in constructing an information security policy. International security standards, for example, ISO/IEC 27002 is an extremely important guide which may be used at the start of the information security policy development process.

The fourth dimension is the **people support** dimension. This dimension includes all the people who are involved in the development of an information security policy. It is essential that management, employees and stakeholders support the entire process of developing and implementing an information security policy if the policy is to survive and attain its objectives.

Lastly, organisations need to use **existing theories** in order to understand the behavioural intention of their employees with regard to information security policy compliance. This study relied on the Theory of Planned Behaviour and General Deterrence Theory in order to understand employees' behavioural intention to comply with the security policies of an organisation.

A survey of 400 security professionals was conducted in order to evaluate the concepts of the framework. The findings are discussed below:

11.7.2 Overall descriptive data analysis findings

Descriptive statistics were used to measure the level of importance of the framework constructs. The mean of all seven constructs was above 3 the middle value in the five-point scale (Dewberry, 2004, p. 14). Accordingly, the results of the descriptive statistics revealed that, in general, the respondents agreed that all seven constructs of the proposed framework were important.

Contrary to the content analysis findings, the overall results of the survey showed that risk assessment was the most important construct of the seven measured constructs. This result is not, however, surprising because the main reason for developing information security policies is to mitigate the various security risks that organisations face. The second most important construct was management support. Management plays a significant role in making decision in an organisation, including decisions regarding budgeting as well as information security policy approval and enforcement. The findings revealed that the respondents also believed that information security policy compliance and employee support were important steps and should be conducted during an information security development and implementation process. The overall results showed that information security policy monitoring was the least important of the seven constructs. This, in turn, implies that this area needs more attention. The content analysis also revealed the same result with information security monitoring showing the lowest frequency of tags as compared to the other categories.

11.7.3 Inferential statistical data analysis findings

As discussed in Chapter 8, the findings showed a positive correlation between management support and information security policy development life cycle constructs with a statistically significant result. In addition, the findings revealed that there is the existence of a relationship with significant influence between employee support and information security policy development life cycle constructs. The next section discusses the limitations and future of this research project.

11.8 Limitations and future research project

The first limitation of this study is related to the demographics of the respondents in the survey. The respondents of the survey were from the United States of America and the United Kingdom only. This may, in turn, constitute a major limitation as regards the generalisability of the study findings. These two countries are developed countries with advanced technology. In the underdeveloped countries there is a lack of a high level of both technology and knowledge and, thus, the two groups may not share the same opinions about the processes proposed in the framework. Nevertheless, the proposed framework should provide guidelines that underdeveloped countries could follow in order to improve their mechanisms for developing information security policies. Future research could involve an empirical study that compared the development of information security policies in underdeveloped and developed countries.

The second limitation is the time and cost that would be involved in implementing all the processes suggested in the proposed framework. As discussed in Chapter 3, the development of information security policies requires that organisations have sufficient budgetary resources to cover all the costs. These costs include, for example, the costs of conducting a risk assessment; information security policy construction; consulting with stakeholders; conducting training and education sessions and the monitoring of users' activities by, perhaps, using an automated monitoring system. Implementing the processes in a large organisation would require considerable time and money as compared to a small organisation. However, as discussed in Chapter 6, the decision to embark on the information security policy construction should be based on the risk appetite that the organisation is willing to take. A cost benefit analysis should inform the organisation if it is worth spending the required amount of resources on the information security policy construction.

The third limitation of the study is the weakness of the content analysis. Silverman (1993) points out that the weakness of content analysis is that it is limited to examining already recorded messages only and it does not show unobtrusive messages. The content analysis conducted in this study involved 21 documents only. There is, thus, little doubt that other information may have been found in documents that were not part of the selected sample.

11.9 Summary

This chapter contains reflections and concluding remarks on the thesis as a whole. The chapter also discusses how the objectives of the study were realised. The research methodology that was followed was revisited. In addition, the chapter highlights the contributions of the study. The chapter also discusses the limitations of the study and proposed possible future research. The study developed a maturity assessment framework that should guide organisations in developing and implementing information security policies. The proposed framework will ensure a comprehensive structured methodology for assessing the maturity level of an information security policy.

Reference List

Abu-Khadra, H.A., Chan, J.O., and Pavelka, D.D. (2012). Incorporating the COBIT Framework for IT Governance in Accounting Education. *Communications of the IIMA*, 12 (2). pp. 19 - 27.

Abdel-Aziz, A. (2010). *How to Review and Assess Information Security Policy: The Six-Step Process*. Retrieved 15 May, 2013 from: http://www.sans.edu/.

Abzug, C., Adams, J., Aldrich, M., Bacoyanis, G., Barret, C., and Bartol, N. (2003). *Systems Security Engineering Capability Maturity Model - SSE-CMM Model Description Document version 3.0*. Pittsburgh, Pennsylvania, USA. Software Engineering Institute, Carnegie Melon University.

Ahmad, A., Guy, G., and Wasana, B. (2011). Developing an IS-impact decision tool: A literature based design science roadmap. *European Conference on Information Systems. Helsinki*.

Ahuja, S,. and Goldman, J.E. (2009). *Integration of COBIT, Balanced Scorecard and SSE-CMM as a strategic Information Security Management (ISM) framework*. Retrieved 10 May, 2014 from: https://www.cerias.purdue.edu/assets/pdf/bibtex_archive/2009-21.pdf.

Ajzen, I.1991. The theory of planned behaviour. *Special Issue: Theories of cognitive self-regulation. Organisation Behavior and Human Decision Processes*, 50 (2), pp. 179 - 211.

Al-Awadi, M., and Renaud, K. (2007). Success factors in information security implementation in organisations. *Proceedings of IADIS International Conference e-Society*, pp. 169 - 176.

Alwi, N.H. (2012). *E-learning Stakeholders Information Security Vulnerability Model*. Published Thesis. Cranfield University. UK.

Amrollahi, A., Ghapanchi, A.H., and Talaei-Khoei, A. (2014). From Artefact to Theory: Ten Years of Using Design Science in Information Systems Research. *In Proceedings of the 13th European Conference on Research Methodology for Business and Management Studies: ECRM 2014, Academic Conferences Limited*.

Anand, V. (2012). Security Policy Management Process within Six Sigma Framework. *Journal of Information Security*, 3 (1), pp. 49 – 58.

Avolio, F.M., Fallin, S., and Pinzon, D.S. (2007). Producing Your Network Security Policy. *WatchGuard Technologies*.

Babbie, E. (2005). *The Basics of Social Research.* Toronto, Canada. Thomson Wadsworth.

Bacik, S. (2008). Building an effective information security policy architecture. *CRC Press, Taylor and Francis Group: Boca Raton.* USA.

Bandura, A. (1977). Self-efficacy: Toward a unifying theory of behavioral change. *Psychological Review,* 84, pp. 122 – 147.

Baskerville, R. (1988*). Designing Information Systems Security*, Chichester: J. Wiley.

Bassey, M. (1990). On the Nature of Research in Education (Part 2). *Research Intelligence*, 37, pp. 39 - 44.

Bayuk, J. (2009). *How to Write an Information Security Policy.* Retrieved 22 May, 2014 from: http://www.computerworld.com/article/2525539/security0/how-to-write-an-information-security-policy.html.

Beccaria, C. (1794). *Classical Theory, Deterrence Theory, Rational Choice Theory, Routine Activities Theory*. Retrieved 12 June, 2014 from: http://www.brianpaciotti.com/lecture%208%20FALL%2005.pdf.

Becker, J., Knackstedt, R., and Pöppelbu, J. (2009). Developing maturity models for IT management – a procedure model and its application. *Business Information Systems Engineering*, 1, pp. 213 – 222.

Björck, F. (2008). *Auditing Information Security Management Systems – Towards a Practical Method*. Retrieved 10 June, 2014 from: http://people.dsv.su.se/~bjorck/files/research-overview.pdf.

Blaikie, N. (2010). *Designing social research (2nd ed.)*. Cambridge: Polity Press.

Blumberg, B., Cooper, D., and Schindler, P. (2008). *Business Research Methods. 2nd European Edition*. London: McGraw –Hill.

Bobek, D. D., Hageman, A. M., and Kelliher, C. F. (2013). Analyzing the Role of Social Norms in Tax Compliance Behaviour. *Journal of Business Ethics*, 115 (3), pp. 451 - 468.

Bonehill, C. (2007). Policy development framework. Retrieved 12 May, 2013 from: https://www.cafcass.gov.uk/media/6755/POLICY%20FRAMEWORKAUG07a.pdf.

Bowen, P.L, Cheung, M.D., and Rohde, F.H. (2007). Enhance IT Governance practices: A model and case study of an organisation's efforts. *International Journal of Accounting Information Systems*, 8 (3), pp. 191 - 221.

Braun, V. and Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3, pp. 77 - 101.

Browne, J.A. (1997). You Can't Manage What You Can't Measure. *Information Technologies for Utilities*, Prentice Hall, New York.

Bulgurcu, B., Cavusoglu, H., and Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Belief and Information Security Awareness. *MIS Quarterly*, 34 (3), pp. 523 - 548.

Bunniss, S., and Kelly, D.R (2010). Research paradigms in medical education research. *Medical Education Journal*, 44, pp. 358 – 366.

BusinessDictionary. (2004) *Definition of statistical analysis*. Retrieved 12 June, 2014 from: http://www.businessdictionary.com/.

BusinessDictionary. (2001). *Definition of binding agreement.* http://www.businessdictionary.com/definition/causal.html.

Cameron, R. (2011). Mixed Methods Research: The Five Ps Framework. *Electronic Journal of Business Research Methods*, 9 (2), pp. 96 - 108.

Canal, V., and Aceituno, V. (2006), *ISM3, Information Security Management Maturity Model*, Version 1.20. Creative Commons.

Cavusoglu, H., Cavusoglu, H., Son, J.Y., and Benbasat, I. (2008). *Information Security Control Resources in Organisations: A Multidimensional View and Their Key Drivers,* UBC Working Paper.

CERT Insider Threat Center, 2014. *2014 U.S. State of Cybercrime Survey.* Retrieved 16 June, 2014 from: http://resources.sei.cmu.edu/asset_files/Presentation/2014_017_001_298322.pdf

Chapin, D. A., and Akridge, S. (2005). *How Can Security Be Measured?* Retrieved 4 March, 2012 from: http://www.isaca.org.

Chen, H., and Li, W. (2014). Understanding organisation employee's information security omission behaviour: an integrated model of social norm and deterrence. *Proceedings of PACIS 2014*, Chengdu, China.

Chia, R. (2002). The Production of Management Knowledge: Philosophical Underpinnings of Research Design. *Essential Skills for Management Research*, London: SAGE Publications Ltd.

Chuvakin, A. (2008). *Five basic mistakes of Security Policy*. Retrieved October 3, 2011, from:http://www.computerworld.com/s/article/9065202/Five_basic_mistakes_of_security_policy.

CitiGroup. (2000). *Secretary of defense Corporate fellows program, Final report*. Retrieved 10 March, 2013 from: http://www.ndu.edu/sdcfp/reports/Citigroup.doc.

Collis, J., and Hussey, R. (2009). *Business Research: A Practical Guide for Undergraduate and Postgraduate Students (3rd.ed)*. New York: Palgrave Macmillan.

Colquitt, J.A., and Zapata-Phelan, C.P. (2007). Trends in theory building and theory testing: A five-decade study of the Academy of Management Journal. *Academy of Management Journal*, 50 (6), pp. 1281 - 1303.

Conner, B., Noonan, T., and Holleyman, R. (2003). *Information Security Governance: Toward a framework for action*. Business Software Alliance. Retrieved 10 March, 2014 from: http://www.bsa.org.

Colwill, C. (2009). Human factors in information security: The insider threat who can you trust these days? *Information security technical report,* 14, pp. 186 – 196.

Control Objectives for Information Technology (COBIT). (2007). *ISACA*. Retrieved 10 May, 2014 from: http://www. isaca.org.

Corley, K.G., and Gioia, D.A. (2011). Building theory about theory building: What constitutes a theoretical contribution? *Academy of Management Review,* 36 (1), pp. 12 - 32.

Corpuz, M.S., and Barnes, P. (2010). Integrating information security policy management with corporate risk management for strategic alignment. *In Proceedings of the 14th World Multi-Conference on Systemics, Cybernetics and Informatics (WMSCI)*, Orlando, Florida.

Creswell, J.W. (2009). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. Sage, Thousand Oakes.

Creswell, J.W. and Plano V.I. (2011). *Designing and Conducting Mixed Methods.* Research Sage, Thousand Oaks.

Crossman, A. (2003*). Descriptive vs. Inferential Statistics*. Retrieved 10 May, 2014 from: http://sociology.about.com/od/Statistics/a/Descriptive-inferential-statistics.htm.

CyberSecurity Watch Survey. (2011). *Organisations Need More Skilled Cyber Professionals to Stay Secure*. CSO magazine.

CyberSecuirtyWatch Survey. (2011). *How Bad Is the Insider Threat?* CSO Magazine, U.S. Secret Service, Software Engineering Institute CERT Program at Carnegie Mellon University and Deloitte.

Cybercrime Survey. 2014. *US State of Cybercrime Survey*. CSO Magazine, U.S. Secret Service, Software Engineering Institute CERT Program at Carnegie Mellon University and Price Waterhouse Cooper.

D'Arcy, J., Hovav, A., and Galletta, D. (2009). User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. *Information Systems Research*, 20 (1), pp. 79 – 89.

Davis, F. (1989). Perceived usefulness, perceived ease of use and user acceptance of information technology. *MIS Quarterly*, 13 (3), pp. 319 - 339.

Davis, F.D. (1986). *A technology acceptance model for empirically testing new end user information systems: Theory and results*. Doctoral dissertation, Massachusetts Institute of Technology. UK.

Davis, F.D., Baggozzi, R.P. and Warshaw, P.R 1989. *User acceptance of computer technology: A comparison of two theoretical models.* Management Science, 35 (8), pp. 982 - 1003.

Denzin N.K, Lincoln Y.S. (2000). *Handbook of Qualitative Research*, 2nd ed. Thousand Oaks, CA: Sage Publications 2000.

De Haes, S., and Van Grembergen, W. (2008). Analysing the Relationship Between IT Governance and Business/IT Alignment. Proceedings of the 41 Hawaii *International Conference on System Science*, 8, pp. 1 - 10.

De Haes, S., and Van Grembergen, W. (2008). *Practices in IT Governance and Business/IT Alignment*. ITAG Research Institute, 6, pp. 1 - 8.

Dewberry, C. (2004). *Statistical Methods for Organisational Research: Theory and Practice*. Psychology Press Business and Economics.

Diver, S. (2007). Information Security Policy – A Development Guide for Large and Small Companies. Retrieved 12 June, 2013 from: http://www.sans.org.

Doughty, K., and Grieco, F. (2005*). IT Governance: Pass or Fail?* Information Systems Audit and Control Association, 6, (12), pp.124 - 132.

Douglas, J. (2011). *Risk Appetite and Tolerance*. Retrieved 12 June, 2013 from: http://www.theirm.org/media/464806/IRMRiskAppetiteExecSummaryweb.pdf.

Duncan, A., Creese, S., and Goldsmith, M. (2012). Insider Attacks in Cloud Computing. *IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications*, 18, pp. 857 - 862.

DTTL, (2011). *Raising the Bar 2011 TMT Global Security Study – Key Findings*. Deloitte. Retrieved 4 March, 2012 from: http://www.deloitte.com.

Dzazali, S., Sulaiman, A., and Zolait, A.H. (2009). Information Security Landscape and Maturity Level: Case Study of Malaysian Public Service (Mps) Organisations. *Government Information Quarterly*, 26 (4), pp. 584 – 593.

Du Preez, R., and Botha, R.A. (2010). *A Model for Green IT Strategy: A Content Analysis Approach*. Published Masters Thesis. Nelson Mandela Metropolitan University. Port Elizabeth, South Africa.

Edwards, G. (2011). *Federal Government Information Systems Security Management and Governance are Pacing Factors for Innovation*. Published Thesis. WALDEN University.

Elo, S., and Kyngäs, H. (2008). The qualitative content analysis process. *Journal of advanced nursing*, 62 (1), pp. 107 - 115.

Eshlaghy, A.T., and Pourebrahimi, A. (2011). Presenting a Model for Ranking Organisations Based on the Level of the Information Security Maturity. *Computer and Information Science*, 4 (1), pp. 21 - 32.

Easterby-Smith, M., Thorpe, R., and Jackson, P. (2008). *Management Research (3rd ed.*). London: SAGE Publications Ltd.

Etsebeth, V. (2006). Information Security Policies – The legal risk of uniformed personnel. Information Security Management and Regulatory Compliance in the South African Health Sector. *Proceedings of the 6th Annual Information Security South Africa Conference*, Sandton, South Africa.

Felton, K. (2010). *Risk appetite or risk analytics: the chicken or the egg*. Retrieved 12 March, 2013 from: www.willis.com.

Ferraiolo, K., and Sachs, J.E. (2000). Distinguishing Security Engineering Process Areas by Maturity Levels. *Proceedings of the Ninth Annual Canadian Information Technology Security Symposium*, Ottawa, Canada.

Funchall, D. (2011). *An adaptive maturity model for small, medium and micro information technology enterprises in South Africa*. Published Doctorate Thesis. Nelson Mandela Metropolitan University, South Africa.

Furnell, S. (2010). Jumping Security Hurdles. *Computer Fraud and Security*, 6, pp. 10 - 14.

Gantz, J.F., and Chute, C., and Manfrediz, A. (2008). *The diverse and exploding digital universe*. IDC White Paper.

GAO, 1989. *Content Analysis: A Methodology for Structuring and Analysing Written Material*. Retrieved 22 March, 2013 from: http://archive.gao.gov/d48t13/138426.pdf.

Gefen, D., Straub, D.W., and Boudreau, M.C. (2000). Structural Equation Modelling and Regression: Guidelines For Research Practice. *Communications of the AIS*, 4, pp. 61 - 77.

Gerber, M., Von Solms, R., and Overbeek, P. (2001). Formalizing information security requirements. *Information Management and Computer Security*, 9 (1), pp. 32 – 37.

Gerber-Nel, C., Nel, D., and Kotze, T. (2003). *Marketing Research*. (M.Cant, Ed.) Pretoria: Van Schaik Publishers.

Gobler, C.P and Von Solms, S.H. (2003*). A model to assess the Information Security status of an organisation with special reference to the Policy Dimension*. Published Masters Thesis. Rand Afrikaans University.

Goel, S,. and Chengalur-Smith, I.N. (2010). Metrics for characterizing the form of security policies. *The Journal of Strategic Information Systems*, 19 (4), pp. 281 – 295.

Griffins, M. (2009). *How to write a policy manual*. Retrieved 14 May, 2014 from: http://www.templatezone.com/download-free-ebook/office-policy-manual-reference-guide.pdf.

Hardy, G., and Williams, P. (2010). Using IT Governance And COBIT To Deliver Value With IT And Respond To Legal, Regulatory And Compliance Challenges. *Information Security Technical Report*, 11 (1), pp. 55 - 61.

Heikkila, F.M., (2009). *An Analysis of the Impact of Information Security Policies on Computer Security Breach Incidents in Law Firms*. Published Thesis. Graduate School of Computer and Information Sciences Nova Southeastern University.

Herath, T., and Rao, H.G. (2009). Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations. *European Journal of Information Systems,* 18 (2), pp. 106 - 125.

Hevner, A.R., March, S.T., and Park, J. (2004). Design Science Research Guidelines. *The Management Information Systems Quarterly*, 28 (1), pp. 75 - 105.

Hevner A.R. (2007). A Three Cycle View of Design Science Research. *Scandinavian JIS*, 19 (2), pp. 87 - 92.

Hoffman, S. (2008). *Corporate Security Policies Found Ineffective*. Retrieved 12 February, 2013 from: http://www.crn.com/news/security/211601180/corporate-security-policies-found-ineffective.htm.

Hong, K.S., Chi, Y.P., Chao, L.R., and Tang,J.H. (2006). An empirical study of information security policy on information security elevation in Taiwan. *Information Management and Computer Security*, 14 (2), pp. 104 – 115.

Hone, K,. and Eloff, J.H.P. (2002). Information Security Policy – what do international security standards say? *Computers and Security,* 21 (5), pp. 18 – 25.

Humphreys, E.J. (1998). *Guide to Risk Assessment and Risk Management*. BSI, London.

IBM-ISF. (2007). *Introducing the IBM security Framework and IBM Security Blueprint to Realize Business - Driven Security Red guides for Business Leaders*. Retrieved 14 June, 2012 from: http://www.redbooks.ibm.com/redpieces/pdfs/redp4528.pdf.

Ifinedo, P. (2012), Understanding information systems security policy compliance: An integration of the theory of planned behaviour and the protection motivation theory. *Computers and Security,* 31 (1), pp. 83 - 95.

Information Security Governance. (2004). *Information Security Governance: A call to action*. Retrieved 15 June, 2014 from: https://www.dhs.gov/sites/default/files/publications/csd-informationsecuritygovernance-acalltoaction-2004.pdf.

InformationShield, 2010. *Regulatory Requirements for Information Security Policies.* Retrieved 15 August, 2014 from: http://www.informationshield.com/securitypolicyregulatoryrequirements.html.

InstantSecurityPolicy.com (2013). *The IT Security Guide: why need one, what it covers, and how to implement it*. Retrieved 14 June, 2012 from: http://www.instantsecuritypolicy.com/Introduction_To_Security_policies.pdf.

ISM3 Consortium. (2007). *Information Security Management Maturity Model version 2.10" Consortium*. Retrieved 14 June, 2012 from: http://www.ism3.com/.

ISO/IEC 21827. (2008). *Information technology – Systems security engineering – Capability Maturity Model Capability Maturity Model (SSE-CMM)*. Retrieved 25 June, 2014 from: http://www. iso.org.

ISO/IEC 27002. (2013). *Code of practice for information security management.* Retrieved 15 June, 2014 from: http://www.bsi-global.org.

ISO/IEC38500. (2008). *Corporate Governance of Information Technology*.

IT Governance Institute. (2005). *IT Governance Domains Practices and Competencies: IT Alignment Who is in Charge?* Rolling Meadows, IL, USA. Retrieved 15 June, 2014 from: www.itgi.Org.

ITGI. (2005), *IT Governance Institute, Control Objectives for Information and related Technology (COBIT)*, Version. 4, USA, Retrieved 10 April, 2013 from: www. itgi.org.

Jarmon, D. (2002). *A Preparation Guide to Information Security Policies.* Retrieved 14 June, 2012 from: http://www.sans.org/reading-room/whitepapers/policyissues/preparation-guide-information-security-policies-503.

Johnston, A.C and Hale, R. (2009). Improved security through Information Security Governance. *Communications of the ACM*, 52 (1), pp. 126 - 129.

Johnson, R.B. and Onwuegbuzie, A.J. (2004). Mixed Methods Research: A Research Paradigm whose Time has Come. *Educational Researcher*, 33 (7), pp. 14 - 26.

Kadam, A.W. (2007). Information Security Policy Development and Implementation. *Information Systems Security*, 16 (5), pp. 246 – 256.

Khalid, K., Abdullah, H. H., and Kumar, M. (2012). Get along with quantitative research process*. International Journal of Research in Management*, 2 (2), pp. 15 - 29.

Kankanhalli, A., Teo, H.H., Tan, B.C., and Wei, K.K. (2003). An Integrative Study of Information Systems Security Effectiveness. *International Journal of Information Management,* 23, pp. 139 - 154.

Karyda, M., Kiountouzis, E., and Kokolakis, S. (2005). Information systems security policies: a contextual perspective. *Computers and Security*, 24 (3), pp. 246 – 260.

Khan, R. (2010). *Practical approaches to organisational information security management*. Retrieved 05 January, 2014 from: http://www.sans.org/reading-room/whitepapers/leadership/practical-approaches-organisational-information-security-management-33568.

King III Report - The Institute of Directors in Southern Africa. (2009). *King Report on Governance for South Africa and the King Code of Principles (King III)*. Retrieved 10 January, 2012 from: http://www.iodsa.co.za/?kingIII.

Korac-Kakabadse, N and Kakabadse, A. (2001). IS/IT Governance: Need for an Integrated Model. *Corporate Governance*, 1 (4), pp. 9 - 11.

Krippendorff, K. (2004). *Content Analysis: An Introduction to its Methodology (2nd ed.)* Sage Publications, Inc.

Kuechler, W., Vaishnavi, V. (2008). On theory development in design science: anatomy of a research project. *European Journal of Information Systems*, 17, pp. 489 – 504.

Kuechler, W., Vaishnavi, V. (2012). A framework for theory development in design science research: multiple perspective. *Journal of the association for information systems*, 13, pp. 3 - 12.

Kuhn, T.S. (1962). *The structure of scientific revolution*: Chicago: University of Chicago Press. USA.

Lee, Y., and Larsen, K.R. (2009). Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-malware software. *European Journal of Information Systems*, 18, pp. 177 - 187.

Leedy, P., and Ormrod, J. (2005). *Practical research: Planning and design* (7th, Ed.) New Jersey: Prentice-Hall.

Lincoln, Y.S., and Guba, E.G. (1982). Epistemological and methodological bases of naturalistic inquiry. *Education Communication Technology*, 30 (4), pp. 233 – 52.

Lineman, D.J. (2009). *The Total Cost of Information Security Policy Management*. Retrieved 25 September, 2013 from: http://www.informationshield.com/papers/TheTotalCostofPolicyManagement.pdf.

Iivari, J. (2007). A paradigmatic analysis of Information Systems as a design science. *Scandinavian Journal of Information Systems*, 19 (2), pp. 39 - 64.

Lohmeyer, D.F., Mccrory, J., and Pogreb, S. (2002). Managing information security policy. *McKinsey Quarterly Special Edition*, 11, pp. 12 - 15.

Lutteroth,C., Reilly, A.L., Dobbie, G., and Hamer, J. (2007). A maturity model for computing education. *Ninth Australasian Computing Education Conference, Conferences in Research and Practice in Information Technology*, 66, (2), pp. 107 - 114.

Mallette, D. (2005). *IT Performance Improvement With COBIT and the SEI CMM*. Retrieved 02 April, 2012 from: http://www.isaca.org/.

Man, T.J,. (2007). *A framework for the comparison of Maturity Models for Project-based Management*. Published Masters thesis. Utrecht University. Netherlands.

Marshall, C., and Rossman, B. (2010). *Designing Qualitative Research.* London: SAGE Publications Ltd.

Mason, J. (2002). *Qualitative researching* (2nd ed.). London: Sage Publications.

Mauritian Computer Emergency Response Team (2011). *Guideline on Information Security Policy*. Retrieved 22 September, 2013 from: http://cert-mu.gov.mu/English/Documents/Guidelines/2011/Guideline%20on%20Information%20Security%20Policy.pdf.

Maynard, S.B. and Ruighaver, A.B. (2006). What Makes A Good Information Security Policy: a preliminary framework for evaluating security policy quality. *In: Proceedings of the fifth annual security conference*, Las Vegas, Nevada USA.

Maynard, S.B., Ruighaver, A.B., and Ahmad, A. (2011). *Stakeholders in security policy development*. Retrieved 18 December, 2013 from: http://ro.ecu.edu.au/ism/125/.

MAXQDA (2012). *Qualitative Data Analysis Software for Mac and Windows.* Retrieved 18 December, 2013 from: http://www.maxqda.com/.

McFadzean, E., Ezingeard, J. and Birchall, D. (2008). Anchoring information security governance research: sociological groundings and future directions. *Journal of Information Systems Security*, 2 (3), pp. 3 - 48.

McKenna, S. (2010). Keeping it real: Updating your security policy. *Information security Journal*, 7 (2), pp. 18 – 21.

Merkow, M., and Johnson, R. (2010). *Security Policies and Implementation Issues*. Jones and Bartlett Learning.

Miller, G.A. (1956). The magical number seven, plus or minus two: Some limits on our capacity for processing information. *Psychological Review*, 63 (2), pp. 81 - 97.

Miller, M. (2008). *Reliability and validity*. Retrieved 28 June, 2013 from: http://www.michaeljmillerphd.com/res500_lecturenotes/reliability_and_validity.pdf.

Mlangeni, S.A., and Biermann, E. (2006). *Assessment of Information Security Policies within the Polokwane Region: A Case Study.* Published Doctoral dissertation, Tshwane University of Technology, South Africa.

Monarch Bank. (2014). *Monarch Bank Code of Conduct*. Retrieved 25 June, 2014 from: https://www.monarchbank.com/pdf/Monarch%20Code%20of%20Conduct.pdf.

Morgan, D.L. (2007). Paradigms Lost and Pragmatism Regained: Methodological Implications of Combining Qualitative and Quantitative Methods. *Journal of Mixed Methods Research*, 1 (1), pp. 48 - 76.

Myyry L., Siponen M., Pahnila S., Vartiainen T., and Vance A. (2009). What levels of moral reasoning and values explain adherence to information security rules? An empirical study. *European Journal of Information Systems*, 18 (2), pp. 126 – 139.

National Computer Board. (2011). *Guideline on Information Security Policy*. Retrieved 08 June, 2013 from: http://www.ncb.mu/English/Documents/Downloads/Reports%20and%20Guidelines/Guideline%20on%20Information%20Security%20Policy.pdf.

National Institute of Standards and Technology Special Publication 800-14. (1996). *Generally Accepted Principles and Practices for Securing Information Technology Systems*. Retrieved 12 June, 2013 from: http://csrc.nist.gov/publications.

National Institute of Standards and Technology Special Publication 800-16, (2013). *A Role-Based Model for Federal Information Technology Cyber Security Training*. Retrieved 22 March, 2013 from: http://csrc.nist.gov/publications.

National Institute of Standards and Technology Special Publication 800-30. (2011). *Risk Management Guide for Information Technology Systems*. Retrieved 09 December, 2013 from: http://csrc.nist.gov/publications/.

National Institute of Standards and Technology Special Publication 800-30. (2012). *Guide for Conducting Risk Assessments*. Retrieved 10 February, 2014 from: http://csrc.nist.gov/publications/.

Nunnally, J.C., and Bernstein, I. (1994). *Psychometric Theory* (3rd ed.), New York: McGraw Hill.

Oates, B. (2006). *Researching Information Systems and Computing*. London: Sage Publications.

OECD, (2004). *Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data.* Retrieved from 12 June, 2014 from: http://www.oecd.org/dsti/sti/it/secur/prod/priv-en.htm.

Offermann, P., Levina, O., Schonher, M., and Bub, U. (2009). *Outline of a Design Science Research Process*. Malvern, PA, United States of America.

Okongwu, U., Morimoto, R., and Lauras, M. (2013). The maturity of supply chain sustainability disclosure from a continuous improvement perspective. *International Journal of Productivity and Performance Management*, 62 (8), pp. 4 - 14.

Olivier, M. (2009). *Information Technology Research* (3rd ed.) Pretoria: Van Schaik Publishers.

Oxford Dictionary (2001). *Definition of assurance.* Retrieved from 12 June, 2014 from: http://www.oxforddictionaries.com/.

Pahnila, S., Siponen, M., and Mahmood, A. (2007). Employees' Behavior towards IS Security Policy Compliance. *Proceedings of the 40th Hawaii International Conference on System Sciences*, pp. 156 – 166.

Parker, D.B. (1998). *Fighting Computer Crime - A New Framework for Protecting Information*. John Wiley and Sons, New York.

Patton, M. (2002). *Qualitative Research and Evaluation Methods*, Sage, Thousand Oakes, California.

Peffers, K., Tuunanen, T, Rothenberger, M.A. and Chatterjee, S. (2007). A Design Science research methodology for information systems research. *Journal of Management Information Systems*, 24 (3), pp. 45 - 77.

Peltier T.R, Peltier J., Blackley, J.A. (2005). *Information security fundamentals*. Auerbach Publications: Boca Raton.

Petch, J., Calverley, G., Dexter, H., and Cappelli, T. (2007). Piloting a Process Maturity Model as an e-Learning Benchmarking Method. *The Electronic Journal of e-Learning*, 5 (3), pp. 49 – 58.

Posthumus, S., Von Solms and R., King, M. (2010). The board and IT Governance : the what, who and how. *South African Journal of Business Management*, 41 (3), pp. 23 – 32.

Pries-Heje, J. and Baskerville, R. (2008). The Design Theory Nexus. *MIS Quarterly*, 32 (4), p 731 - 755.

Pullen, W. (2007). The maturity of maturity model research: A systematic mapping study. *Information and Software Technology*, 46, pp. 9 – 15.

Q:PIT (2006). CMMI, SOX and COBIT. *European SEPG*. Retrieved from 22 September, 2013 from: http://www.qpit.net/papers/cmmi-sox-cobit.html.

Raerd (2011). *Descriptive and Inferential Statistics*. Retrieved from 09 January, 2013 from: https://statistics.laerd.com/statistical-guides/descriptive-inferential-statistics.php.

Raerd (2012). *Cronbach's Alpha (α) using SPSS*. Retrieved from 30 March, 2014 from: https://statistics.laerd.com/spss-tutorials/cronbachs-alpha-using-spss-statistics.php.

Raerd (2013). *Cronbach's alpha using Minitab*. Retrieved from 25 June, 2014 from: https://statistics.laerd.com/minitab-tutorials/cronbachs-alpha-using-minitab.php.

Ramanathan RR. (2004). *Information security top-down.* Retrieved from 12 June, 2014 from: http://www.securitymagazine.com/Articles/Feature_Article/61f65404864d8010VgnVCM100000f932a8c0.

Randall, W. S. (2007). *An empirical examination of service dominant logic: The theory of the network.* Published Doctoral dissertation, University of North Texas.

Remenyi, D., Williams, B., Money, A. and Swartz, E. (1998). *Doing Research in Business and Management: An Introduction to Process and Method*. London: Sage.

Rezgui,Y. and Marks, A. (2008). Information security awareness in higher education: An exploratory study. *Computers and security*, 27 (2), pp. 41 – 53.

Richardson, R. (2009). CSI computer crime and security survey. Retrieved from 28 November, 2013 from: http://i.cmpnet.com/v2.gocsi.com/pdf/CSIsurvey2008.pdf.

Robson, C. (2002). *Real World Research: A Resource for Social Scientists and Practitioner-Researchers*, 2nd Ed, Blackwell Publications, Oxford.

RSA Security Inc. (2009). *A Guide to Security Policy - A Primer for Developing an Effective Policy*. Retrieved from 30 November, 2013 from: www.sans.org/security-resources/policies/Policy_Primer.pdf

Sajko, M. (2010). *Measuring and evaluating the effectiveness of Information Security*. Retrieved from 14 February, 2013 from: htttp://www.academypublish.org/papers/pdf/310.pdf.

Sarbanes-Oxley Act Summary. (2002). *Sarbanes-Oxley Act Information Guide*. Retrieved from 14 November, 2013 from: http://www.sarbanes-oxley-compliance.us/.

Saunders, M., Lewis, P., and Thornhill, A. (2009). *Research Methods for Business Students* (5th ed.). Harlow: Pearson Education Limited.

Schultz, E.E. and Shumway, R. (2001). Incident Response: A Strategic Guide for System and Network Security Breaches. Indianapolis, IN: New Riders.

Security Architecture. (2008). *Security policy*. Retrieved from 20 November, 2013 from: http://securityarchitecture.com/docs/Security_Policy.pdf.

Sharp, J.H. (2008). *Globally distributed agile teams: An exploratory study of the dimensions contributing to successful team configuration*. Doctoral dissertation, University of North Texas. USA.

Shayan, A., Soheili, K,. and Abdi, B. (2009). Human Excellence in Information Security: A Complexity Theory Perspective. *Proceedings of the Third International Symposium on Human Aspects of Information Security and Assurance (HAISA).* pp. 36 – 49.

Silverman, J. (1993). *An introduction to content analysis*. Retrieved from 25 January, 2013 from: http://depts.washington.edu/uwmcnair/chapter11.content.analysis.pdf.

Simon, M.K. (2011). *Validity and reliability in qualitative studies*. Dissertation and scholarly research. Seattle, WA, Dissertation success, LLC.

Siponen M., and Vance A. (2010). Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations. *MIS Quarterly* 34 (3), pp. 487 – 502.

Software Engineering Institute, 2006. *CMMI for development, version 1.2: Improving processes for better products*. Retrieved from 25 January, 2013 from: http://www.sei.cmu.edu/publications/.

SSE-CMM. (2003). *Systems Security Engineering Capability maturity Models (SSE-CMM)* ver.3. Retrieved from 21 April, 2013 from: http://www.ssecmm.org/docs/ssecmmv3final.pdf.

Stemler, S. (2001). An Overview of Content Analysis. Practical Assessment, Research and Evaluation, 7 (17).

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

Szuba, T. (1998). *Safeguarding your Technology: Practical Guidelines for Electronic Education Information Security*. Retrieved from 19 January, 2013 from: http://nces.ed.gov/pubs98/98297.pdf.

Talbot, S., and Woodward, A. (2009). Improving an organisations' existing information technology policy to increase security. *Proceedings of the 7th Australian Information Security Management Conference*, 8, pp. 120 - 128.

Tavakol, M. and Dennick, R. (2011). Making sense of Cronbach's alpha. *International Journal of Medical Education*, 2, pp. 53 - 55.

Tech4Law. (2009). *Developing a security policy*. Retrieved from 25 March, 2013 from: http://www.tech4law.co.za/tech-advisor/white-papers/developing-a-security-policy.html.

The International Standards of Supreme Audit Institutions, ISSAI. (1995). *Information System Security Review Methodology*. Retrieved from 20 June, 2013 from: http://www.intosai.org/.

Thomson, K.L. and Solms, R.V. (2006). Towards an Information Security Competence Maturity Model. *Computer Fraud and Security*, 12 (6), pp. 11 - 15.

Tokhid, M.T., Abdul Rashid, A., and Abdul Roni, R. (2012). Exploring the approaches in Malaysian 100 Top Corporate Governance companies. *In Proceedings of the 3rd International Conference on Business and Economic Research (ICBER)*, pp. 3081 – 3106.

Trochim, W. (2006). *What is Research Design? Research Methods Knowledge Base*. Retrieved 3 June, 2012 From: http://www.socialresearchmethods.net/kb/desintro.php.

University of Newcastle (2009). *Policy Development and Review process - Guideline*. Retrieved 12 June, 2014 from: http://www.newcastle.edu.au/Resources/Divisions/Services/Corporate%20Governance/Policy/Policy-Development-Guideline.pdf.

Upadhyaya, P. (2013). *Research methodology*. Retrieved 10 May, 2014 from: http://shodhganga.inflibnet.ac.in/bitstream/10603/6582/13/13_chapter4.pdf.

Vaishnavi, V., and Kuechler, W. (2008). *Design Science Research Methods and Patterns: Innovating Information and Communication Technology*. Florida: Auerbach Publications.

Van Biljon, J.A. (2006). *A model of representing the motivational and cultural factors that influence mobile phone usage facility*. Published Doctorate Thesis, University of South Africa, Pretoria, South Africa.

Van Grembergen, W. (2008). *Practices in IT Governance and Business/IT Alignment. Information Systems Audit and Control Association*. Retrieved 12 June, 2014 from: www.isaca.org.

VanGrembergen, W. (2007). Introduction to the minitrack IT Governance and its Mechansims*. Proceedings of the 40th Hawaii International Conference on System Sciences (HICSS)*.

Verizon RISK Team (2012). *Data breach investigations report*. Retrieved 12 June, 2014 from: http://www.wired.com/images_blogs/threatlevel/2012/03/Verizon-Data-Breach-Report-2012.pdf.

Verma D. (2000). *The generic provisioning problem*. Retrieved 20 March, 2013 from: http://www.informit.com/articles/article.aspx?p=130819.

Voce, A. (2005). *Qualitative Research and Evaluation Methods.* (3rd ed.). Sage Publications. USA.

Von Solms, B., and Von Solms, R. (2005). From Information Security to business security? *Computers and Security*, 24 (4), pp. 271 - 273.

Von Solms, B., and Von Solms, R. (2006). Information Security Governance: A model based on the Direct–Control Cycle. *Computers and Security,* 25 (6), pp. 408 - 412.

Von Solms, R., Thomson, K.L., and Maninjwa, P.M. (2011). Information security policy governance through comprehensive policy architectures. *In Proceedings of the Information Security for South Africa Conference*, 12, pp. 1 - 6.

Von Solms, S.H., and Von Solms, R. (2009). *Information Security Governance,* pp. 87-100. New York: Springer.

Wahsheh, L.A., and Alves-Foss, J. (2008). Security Policy Development: Towards a Life-Cycle and Logic-Based Verification Model. *American Journal of Applied Sciences*, 5 (9), pp. 1117 - 1126.

Walsham, 1995. The Emergence of Interpretivisim in IS Research. *Information System Research*, 6, pp. 12 - 19.

Warman, A.R. (1992). Organisational Computer Security Policy: The Reality. *European Journal of Information Systems*, 1 (5), pp. 305 - 310.

Webber, R. (2012). Evaluating and Developing Theories in the Information Systems Discipline. *Journal of the Association for Information Systems*, 13 (1), pp. 1 - 30.

Webster Dictionary, 2001. *Definition of paradeigma*. Retrieved 28 December, 2013 from: http://www.merriam-webster.com/.

Whetten, D. (1989). What Constitutes a Theoretical Contribution? Academy of Management Review, 14 (4), pp. 486 – 489.

Whitman, M.E and Mattord, H.J. (2008). Management of information security, second edition. Course Technology Cengage Learning: USA.

White, M.D., and Marsh, E. (2006). *Content Analysis: A Flexible Methodology*. Retrieved 20 March, 2013 from: https://www.sfu.ca/cmns/courses/marontate/2010/801/1-Readings/White%20and%20Marsh%20Content%20analysis.pdf.

Williams, P.A. (2007). Information governance: A model for security in medical practice. *Journals of Digital Forensics, Security and Law*, 2 (1), pp. 57 - 72.

Wood, C. (2011). *The Importance of Defining and Documenting Information Security Roles and Responsibilities*. InformationShield, Inc.

Woodhouse, S. (2008). An ISMS (Im)-Maturity Capability Model. Computer and Information Technology Workshops. CIT Workshops. *IEEE 8th International Conference*, 8 (9), pp. 242 – 247.

Workman, M., Bommer, W.H., and Straub, D. (2008). Security Lapses and the Omission of InformationSecurity Measures: A Threat Control Model and Empirical Test. *Computers in Human Behavior,* 24 (6), pp. 2799 - 2816.

Yayla, A. (2011). Controlling insider threats with information security policies. *In proceedings of 19th European Conference on Information Systems: ECIS*, Helsinki, Finland, 9 (12), pp. 242 - 257.

Yin, R.K. (2003). *Case Study Research: Design and Methods* (3rd ed.). California: SAGE Publications.

Appendix A: Ethical clearance

University of Fort Hare
Together in Excellence

ETHICAL CLEARANCE CERTIFICATE

Certificate Reference Number:	FLO021STUY01
Project title:	**A process maturity assessment model of information security policy development life cycle**
Nature of Project:	PHD
Principal Researcher:	Tite Tuyikeze
Supervisor:	Prof S Flowerday
Co-supervisor:	

On behalf of the University of Fort Hare's Research Ethics Committee (UREC) I hereby give ethical approval in respect of the undertakings contained in the above-mentioned project and research instrument(s). Should any other instruments be used, these require separate authorization. The Researcher may therefore commence with the research as from the date of this certificate, using the reference number indicated above.

Please note that the UREC must be informed immediately of

- Any material change in the conditions or undertakings mentioned in the document
- Any material breaches of ethical undertakings or events that impact upon the ethical conduct of the research

The Principal Researcher must report to the UREC in the prescribed format, where applicable, annually, and at the end of the project, in respect of ethical compliance.

Special conditions: Research that includes children as per the official regulations of the act must take the following into account:

Note: The UREC is aware of the provisions of s71 of the National Health Act 61 of 2003 and that matters pertaining to obtaining the Minister's consent are under discussion and remain unresolved. Nonetheless, as was decided at a meeting between the National Health Research Ethics Committee and stakeholders on 6 June 2013, university ethics committees may continue to grant ethical clearance for research involving children without the Minister's consent, provided that the prescripts of the previous rules have been met. This certificate is granted in terms of this agreement.

The UREC retains the right to

- Withdraw or amend this Ethical Clearance Certificate if
  - Any unethical principal or practices are revealed or suspected
  - Relevant information has been withheld or misrepresented
  - Regulatory changes of whatsoever nature so require
  - The conditions contained in the Certificate have not been adhered to
- Request access to any information or data at any time during the course or after completion of the project.
- In addition to the need to comply with the highest level of ethical conduct principle investigators must report back annually as an evaluation and monitoring mechanism on the progress being made by the research. Such a report must be sent to the Dean of Research's office

The Ethics Committee wished you well in your research.

Yours sincerely

Professor Gideon de Wet
Dean of Research

09 December 2013

Appendix B: Questionnaire

Survey to assess the importance of information security policy development and implementation processes

1. Name of country:
2. Organisation type (Government, Industrial, Banking, Education, Others: please specify)
3. Occupation
A- CIO,
B- Security specialist,
C- IT manager,
D- Others (specify)
4. How many employees work in your organisation? Less than 500; between 500 and 1000; between 1000 and 5000; 5000 – 10 000; > 10 000
5. Does your organisation have an information security policy?
(Answer:
Yes
or No):

How **important** do you believe the following factors are for the successful implementation of Information security policy in your organisation? Where **1) is Not important, 2) Somewhat important, 3) Neutral, 4) Important and 5) is Very important.**

	1	2	3	4	5
6. Visible support and commitment from the top executive management.					
7. A clear understanding of the organisation's security risks.					
8. The information security policy writing process is based on the findings and the recommendations of the risk assessment process.					
9. A suitable information security policy training and education during the information security policy implementation stage.					
10. Regularly assess and monitor the information security policies to ensure that they are effective.					
11. Effective information security policy compliance mechanisms to ensure that employees adhere to organisation's information security policy requirements.					
12. Ensure that employees support and understand their roles and responsibilities of the information security policy requirements.					

Assessment of the information security policy development process

In order to have an effective information security policy, an organisation should select a set of processes to be implemented accurately and to give good results. Please indicate the importance of each of the following security policy development processes where

1) is Not important, 2) Somewhat important, 3) Neutral, 4) Important and 5) is Very important.

Risk assessment processes

	1	2	3	4	5
13. Develop a risk assessment plan that includes the identification of assets to be protected.					
14. Develop a risk assessment plan that includes the assessment of vulnerabilities and security threats.					
15. Security policy is constructed based on the findings of the risk assessment result.					
16. Identify all legal and regulatory requirements pertaining to the organisations.					

Please add any activity that you feel is important with respect to the risk assessment process within your organisation:

Information security policy construction processes

	1	2	3	4	5
17. At the strategic level, develop high level policies which are a set of management mandates that show how executive management plan to protect the organisation's information assets.					
18. At the tactical level, develop detailed security policies which are detailed statements of strategic level policies showing what should be done to comply with the security policy.					
19. At the operational level, develop lower level security policies which define the procedures, plans or processes that address the details of how to perform a specific action.					
20. Organisations' stakeholders must be consulted before the information security policy is submitted to senior management for final approval.					

Please add any activity that you feel is important with respect to the security policy construction process within your organisation:

Information security policy implementation processes

	1	2	3	4	5
21. Different business communication (notices, posters, newsletters, etc.) are used to promote security policy awareness.					
22. There are mechanisms to train all stakeholders so that they understand their responsibilities towards the security policy requirements.					
23. Clearly define the roles of various organisation stakeholders (executive management, information security officials, everyone).					
24. There are mechanisms to educate employees about the new information security policy requirements.					

Please add any activity that you feel is important with respect to the security policy implementation process within your organisation:

Information security policy monitoring processes

	1	2	3	4	5
25. Review the information security policy on a regular basis to make sure that the latest threats and new regulations are kept up to date					
26. Use of automated review scheduling system which alerts when major changes have occurred to existing practices.					
27. Review the audit information to identify the area of frequent security policy deviation.					
28. An established information security policy review and update process exists.					

Please add any activity that you feel is important with respect to the security policy assessment and monitoring process within your organisation:

Management support

	1	2	3	4	5
29. The involvement of executive management in the information security policy development is crucial to the approval of the security policies.					
30. Top management plays a significant role in enforcing the information security policy so as to ensure that employees regard the policy requirements in a serious light.					
31. Executive management is involved in the whole process of information security policy development.					
32. Executive management must have sufficient budget for information security policy development.					

Please add any activity that you feel is important with respect to the management support process within your organisation:

Employee support

	1	2	3	4	5
33. There should be mechanisms to punish employees who intentionally violate the information security policy.					
34. Employees should sign off that they have received and reviewed the policies and agree to be bound by them.					
35. Job termination should be considered for employees who repeatedly violate the information security policy.					
36. Employees that have been trained and are aware of information security policy requirements are likely to comply with such information security policy.					

Please add any activity that you feel is important with respect to the employee support process within your organisation:

Information security policy compliance

	1	2	3	4	5
37. An employee's positive attitude towards compliance with the organisation's information security policy positively influences his/her intention to comply with the requirements of the information security policy.					
38. An employee's perceived social pressure about his/her compliance with the requirements of the information security policy positively influences his/her intention to comply with the requirements of the information security policy.					
39. An employee's perceived benefit of compliance with the organisation's information security policy will positively influence his/her attitude towards complying with the requirements of the information security policy.					
40. An employee's judgment of his/her own knowledge in complying with the requirements of the information security policy positively influences his/her intention to comply with the requirements of the information security policy					

Please add any activity that you feel is important with respect to the information security policy compliance process within your organisation: