UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

A FRAMEWORK AND MODEL OF OPERATION FOR ELECTRONIC PERSONAL INFORMATION TO ACHIEVE AND MAINTAIN COMPLIANCE WITH CONDITION 7 OF THE PROTECTION OF PERSONAL INFORMATION (POPI) ACT

by

PRITTISH DALA

Submitted in fulfilment of the requirements for the degree

PHILOSOPHIAE DOCTOR

in the subject of

INFORMATION TECHNOLOGY

in the

FACULTY OF ENGINEERING, BUILT ENVIRONMENT AND INFORMATION TECHNOLOGY

at the

UNIVERSITY OF PRETORIA

MARCH 2017

Supervisor

PROF H. VENTER

ABSTRACT

Privacy entails controlling the use and access to place, location and personal information. In South Africa, the first privacy legislation in the form of the Protection of Personal Information (POPI) Act (Act 4 of 2013) was signed into law on 26 November 2013. The POPI Act promotes the protection of personal information by South African institutions and specifies the minimum requirements in 12 Chapters, which includes 8 Conditions for lawful processing of personal information. Condition 7 of the POPI Act makes specific provision for security safeguards to ensure the confidentiality and integrity of personal information. While the legislative requirements of Condition 7 of the POPI Act are spelt out in Sections 19, 20, 21 and 22, the requirements are not supported by specific guidance in terms of how these should be satisfied. There is also no specific guidance on the security safeguards, as required in Section 19, to ensure the confidentiality and integrity of personal information. Hence, this thesis - which focuses on electronic personal information - proposes a framework that includes a selection of security safeguards that may serve as a frame of reference and be used by South African institutions that store, process and transmit electronic personal information, to achieve and maintain compliance with Condition 7 of the POPI Act. As part of this study, a POPI research survey is used to assess the current state of security safeguards in South African institutions and to validate the selection of security safeguards of the proposed framework. In addition, a model of operation of security safeguards is proposed to guide one on how the selection of security safeguards should be implemented to achieve and maintain confidentiality and integrity of electronic personal information as required by Condition 7 of the POPI Act. Furthermore, this thesis explores the concept and principles of privacy as well as the importance of privacy and provides an overview of the global privacy legislative landscape, including South African privacy legislation. An analysis is also conducted to assess the extent to which the privacy legislation of the European Union (EU) and South Africa addresses the international 2013 Organisation for Economic Co-operation and Development (OECD) guidelines. The POPI research survey is also used to assess the level of compliance with the POPI Act and specifically Condition 7 of the Act. In addition, the POPI research survey is used to assess the financial value associated with electronic personal information and the potential impact of a data breach of electronic personal information.

SUMMARY

Title: A Framework and Model of Operation for Electronic Personal Information to Achieve and Maintain Compliance with Condition 7 of the Protection of Personal Information (POPI) Act.

Candidate: Prittish Dala.

Supervisor: Professor Hein Venter.

Department: Department of Computer Science.

Faculty: Faculty of Engineering, Built Environment and Information Technology.

Degree: Philosophiae Doctor.

Keywords: Compliance, Confidentiality, Data Protection Directive, Electronic Personal Information, Information Security, Integrity, OECD, POPI Act, POPI Research Survey, Privacy, Protection of Personal Information, Security Safeguards.

I dedicate this thesis to my daughter Ayana Dala, an absolute blessing and joy, who was born during the course of this remarkable journey. In addition, I dedicate this thesis to South African institutions, whom I hope will benefit from this research in tackling the mammoth task of ensuring confidentiality and integrity of electronic personal information.

ACKNOWLEDGEMENTS

I would like to acknowledge and express my sincere appreciation to the following people and institutions for the support received during formulation and completion of this thesis:

- God - Thank you for providing me with the opportunity and strength to undertake and complete this remarkable journey.
- My wife, Renusha Dala - Thank you for providing me with the inspiration and unwavering support to make this thesis a reality, it would not have been possible without you.
- My parents, Vinesh and Hursula Dala - Thank you for all your sacrifices that has afforded me access to the greatest asset, education, and for your continued support and encouragement throughout all my academic endeavours.
- Grandparents, brothers, family members, professional colleagues, friends - Thank you for your support.
- Nina Bhaktawar - Thank you for always availing yourself despite the circumstances to assist me with language editing of this thesis as well as the associated research publications.
- Professor Hein Venter - Thank you for your excellent guidance, assistance and continued inspiration throughout this thesis and associated research publications as well as the financial support for conferences.
- Research survey participants - Thank you for contributing to this research effort by completing the research survey and providing invaluable insights and for those of you who had shared the research survey link with other participants to complete the research survey.
- South African Chapter of Information Systems Audit and Control Association (ISACA) - Thank you for assisting with the distribution of the research survey link to members of the South African chapter of ISACA.
- CIBECS - Thank you for assisting with the distribution of the research survey link to participants who were targeted for the 2012 State of Business Data Protection in South Africa survey.

“Stay Hungry. Stay Foolish.” - Steve Jobs (1955 - 2011).

CONTENTS

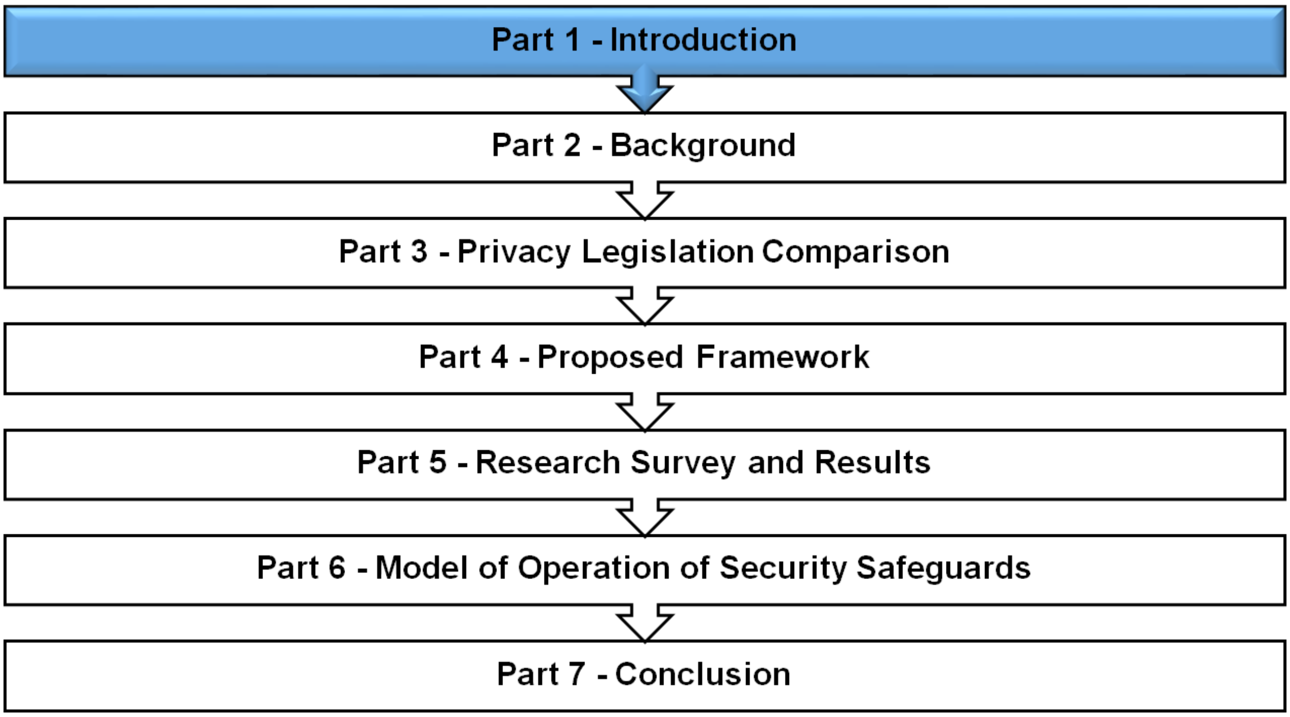
LIST OF ABBREVIATIONS

COBIT	- Control Objectives for Information and related Technology
DLP	- Data Loss Prevention
EU	- European Union
GCIS	- Government Communication and Information Services
IRS	- Internal Revenue Service
ISACA	- Information Systems Audit and Control Association
ISMS	- Information Security Management System
ISO	- International Organisation for Standardisation
NIST	- National Institute of Standards and Technology
OECD	- Organisation for Economic Co-operation and Development
OGUK	- Office of Government Commerce United Kingdom
PCI-DSS	- Payment Card Industry - Data Security Standard
PDCA	- Plan-Do-Check-Act
PIPEDA	- Personal Information Protection and Electronic Document Act
POPI	- Protection of Personal Information
SIEM	- Security Incident Event and Monitoring
US	- United States
USA	- United States of America

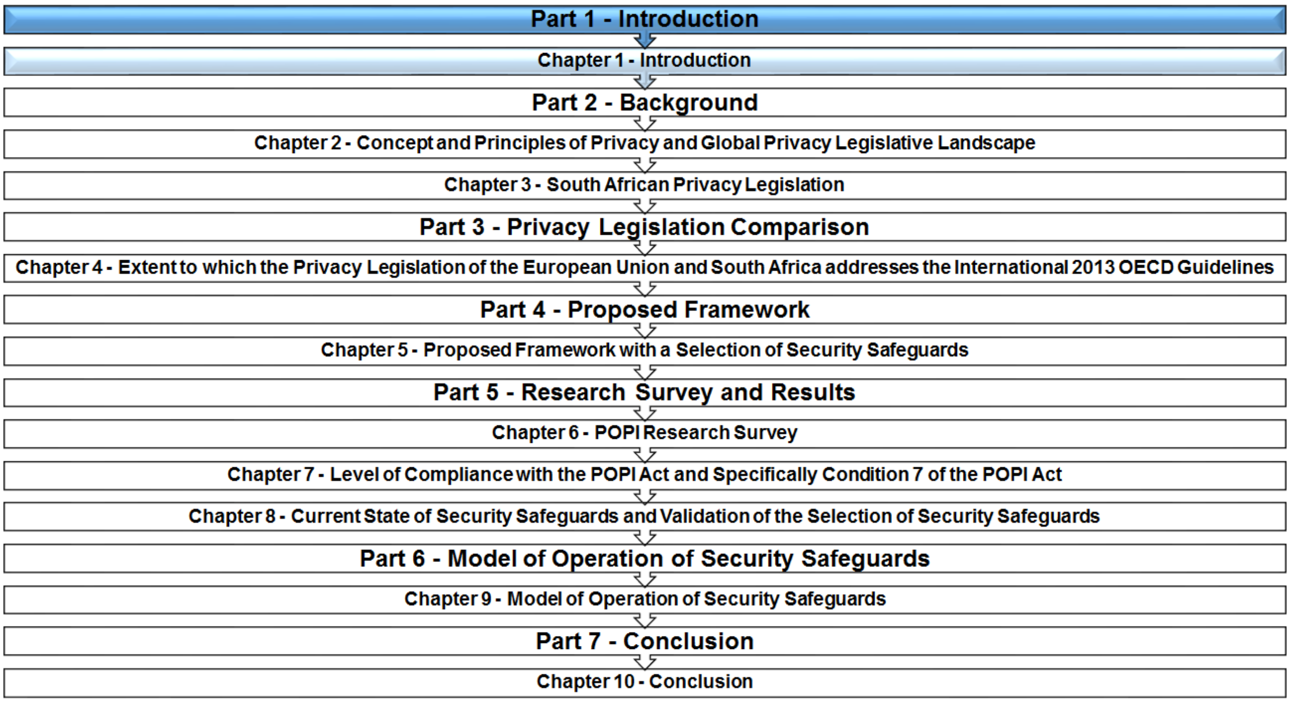
LIST OF TABLES

LIST OF FIGURES

PART 1 - INTRODUCTION


Part 1 - Introduction
Part 2 - Background
Part 3 - Privacy Legislation Comparison
Part 4 - Proposed Framework
Part 5 - Research Survey and Results
Part 6 - Model of Operation of Security Safeguards
Part 7 - Conclusion

CHAPTER 1 - INTRODUCTION



Part 1 - Introduction

Chapter 1 - Introduction

Part 2 - Background

Chapter 2 - Concept and Principles of Privacy and Global Privacy Legislative Landscape

Chapter 3 - South African Privacy Legislation

Part 3 - Privacy Legislation Comparison

Chapter 4 - Extent to which the Privacy Legislation of the European Union and South Africa addresses the International 2013 OECD Guidelines

Part 4 - Proposed Framework

Chapter 5 - Proposed Framework with a Selection of Security Safeguards

Part 5 - Research Survey and Results

Chapter 6 - POPI Research Survey

Chapter 7 - Level of Compliance with the POPI Act and Specifically Condition 7 of the POPI Act

Chapter 8 - Current State of Security Safeguards and Validation of the Selection of Security Safeguards

Part 6 - Model of Operation of Security Safeguards

Chapter 9 - Model of Operation of Security Safeguards

Part 7 - Conclusion

Chapter 10 - Conclusion

1.1 INTRODUCTION

Today, more than ever, we find ourselves in an information revolution that has transformed the way we transact and conduct business, resulting in an unparalleled proliferation of records preserved within databases containing fertile fields of personal data (Solove, 2004). According to the National Crime Prevention Council (2016): “Since its beginning in the 1990s, the Internet has grown into a vast electronic network that now spans the entire globe, and it will only continue to grow. Because people use the Internet in their everyday lives, they rely on it for a safe and accurate exchange of information. Constantly, personal data such as social security numbers, credit card numbers, and passwords are traveling through wires, and also through the air, from one computer to another. With security measures in place to protect this sort of information online, most people feel safe on the Internet and trust that their personal information will remain confidential. But, unfortunately, criminals have also adapted to advancements in technology and, these days, people are becoming victims of crimes committed over the Internet.”

The currency of the digital world and “oil” of the Internet is personal information (Kuneva, 2009). Personal information according to the Organisation for Economic Co-operation and Development (OECD) (2013) is regarded as any information relating to an identifiable, living and natural individual. Personal information can be bought, sold and traded creating economic value (Ali et al., 2013).

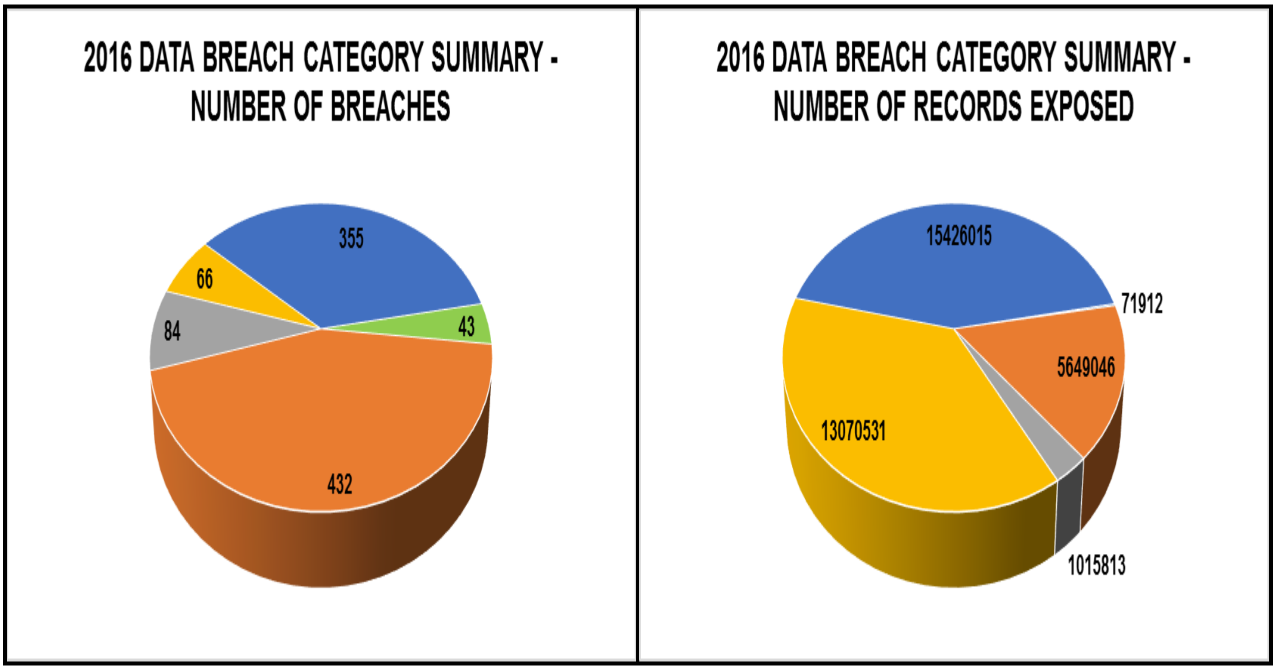
Hence, the global risks identified by the World Economic Forum (2014, 2015, 2016 and 2017) from 2014 to 2017 include data loss as a result of data fraud or theft as a major risk within the technology domain. Furthermore, for the first time in 2017, since 2007, is a massive incident of data fraud/theft listed in the top 5 global risks in terms of the probability by the World Economic Forum (2017).

The value of personal information has increased significantly due to the advent of the information age (Saunders and Zucker, 1999) and this has subsequently resulted in the most prevalent crime of the new millennium known as identity theft (Hoar, 2001). Identity theft is defined by the OECD (2009) as a form of crime which, “occurs when a party acquires, transfers, possesses, or uses personal information of a natural or legal person in an unauthorized manner, with the intent to commit, or in connection with, fraud or other crimes”. Similarly, according to Schipke (2006) identity theft, “involves stealing another person’s “identity” - personal and financial information - for the purpose of committing other crimes constituting fraud.” This rampant form of crime is largely achieved through techniques such as phishing (luring victims to divulge personal information via deceptive emails or fake web sites) and pharming (redirecting victims from an authentic web site to a fraudulent web site which replicates the authentic web site in appearance with the intention to illicit personal information from victims) that are used to trick victims to divulge personal information for illicit purposes (OECD, 2009). The magnitude of this ever increasing prevalent crime is indicated in the *2016 Identity Fraud Study* (Javelin, 2016) that assessed the financial impact of identity theft for a 6-year period ending 2015, at 112 billion U.S. dollars, which is equivalent to 35600 U.S. dollars per minute for the aforementioned period.

Furthermore, criminals break into information systems of institutions to gain unauthorised access to databases, commonly referred to as a data breach, which provides them with the ability to steal personal information such as, among others, financial account numbers, addresses or identity numbers (Information Systems Audit and Control Association (ISACA), 2014a).

The *World’s Biggest Data Breaches* by Information Is Beautiful (2017) provides a graphically illustration of data breaches and globally the number of data breaches and the extent of the data breach in terms of the number of personal information records have both progressively increased on an annual basis from 2004 to 2017. Appendix A provides a summary of numerous high profile data breaches experienced in recent times on a global level by international institutions such as Ashley Madison, Sony Entertainment and the Korean Pharmaceutical Information Centre (Internet Society, 2016) as well as LinkedIn, the Philippine Commission on Elections and Yahoo (Identity Force, 2016).

This growing trend of data breaches is further confirmed by the *2016 Internet Security Threat Report* (Symantec, 2016), which reported 318 (429 million identities exposed) data breaches in 2015 compared to 253 (552 million identities exposed) and 312 (348 million identities exposed) data breaches in 2013 and 2014 respectively. Similarly, from 1 January to 13 December 2016, the Identity Theft Resource Centre (2016) reported a total of 980 data breaches which exposed over 35 million records across several industry sectors as illustrated in Figure 1.1 below.



Category	**Number of breaches**	**Number of records exposed**
Banking/Credit/Financial	43	71912
Business	432	5649046
Educational	84	1015813
Government/Military	66	13070531
Medical/Healthcare	355	15426015
Total	**980**	**35233317**

Figure 1.1: 2016 Data Breach Category Summary

Source: Adapted from Identity Theft Resource Centre (2016)

From a South African perspective, the reporting of data breaches by South African institutions is limited to the extent that only 5 data breaches were registered in 2015

(Gemalto, 2015). The non-reporting of data breaches in South Africa is due to the lack of privacy legislation compelling South African institutions to notify the public in the event of a data breach (Alfreds, 2016). In 2016, the non-reporting of data breaches by South African institutions continued, however the following data breaches became public knowledge:

- Armscor - Invoicing information displaying customer and supplier details exposed (MyBroadBand, 2016a).
- Government Communication and Information Services (GCIS) - Personal information associated with 1500 government employees exposed, including names, phone numbers, e-mail addresses and hashed passwords (Vermeulen, 2016a).
- Department of Water Affairs - Highly sensitive financial data, names of managers and details of projects exposed (Vermeulen, 2016b).
- Ethekwini Municipality - Personal information associated with 98330 residents exposed, including passwords, full names, addresses, and identity numbers (MyBroadBand, 2016b).
- MTN - Names, numbers and bills of customers made accessible to other customers (MyBroadBand, 2016c).

Due to the instrumental value associated with privacy (Moor, 1997), the data breach trend will continue to increase, locally in South Africa and internationally, in terms of the number of data breaches and the extent of personal information exposed. As a result, legislation in the ambit of protecting personal information is critical to preserve the privacy of individuals, which according to Moore (2008), entails controlling the use and access to place, location and personal information. Furthermore, protection of personal information legislation would protect individuals against identity theft as well as offer wide-ranging benefits to institutions including the protection of an institution’s brand, image and reputation, enhancing the credibility of an institution as well as promoting consumer confidence and goodwill (Titus, 2011). Specifically in the South African context, privacy legislation will enhance transparency and end attempts by institutions to keep data breaches under the radar (Floor, 2015).

Countries around the world such as Canada and the United States of America (USA) as well as member states of the European Union (EU) have identified the importance of protecting personal information and as such have implemented privacy legislation with a specific focus on protecting personal information. The EU adopted the Data Protection Directive (also known as Directive 95/46/EC) of 1995 to protect personal information of individuals within member states (European Parliament, 1995). The USA responded to meet the requirements of the Data Protection Directive (1995), specifically relating to the adequacy standard, by introducing the Safe Harbor Act of 2000 designed to allow for the transfer of personal information between EU member states and the USA (Steinke, 2002). Similar to the EU, Canada has the Personal Information Protection and Electronic Document Act (PIPEDA) of 2000 in place to govern how institutions collect, use and disclose personal information (Government of Canada, 2014).

The South African response to the protection of personal information legislation has taken the form of the Protection of Personal Information (POPI) Bill, which was first published for comment in 2005 (Stein, 2012). After undergoing numerous reviews, the POPI Bill (2009) was finally enacted and signed into law on 26 November 2013 as the POPI Act (Act 4 of 2013). This thesis commenced in 2014 and at the time of completing the thesis, the POPI Act (2013) was still not enforced and the commencement date was still to be announced.

This chapter serves as an introduction to the thesis and also provides the motivation for undertaking the study. Furthermore, this chapter provides the research problem and associated research questions as well as the research goal, scope, limitations, objectives, methodology and layout. In addition, a listing is provided of the research work associated with this thesis, which has already been published as research papers as part of conference proceedings and formulated to be submitted to a journal for consideration to be published.

1.2 MOTIVATION

As highlighted in the introduction of this chapter, there was a need for protection of personal information legislation in South Africa, which eventually came to the fore in 2013 when it was enacted in the form of the POPI Act (2013). This thesis is motivated by Condition 7 of the POPI Act (2013) in the context of electronic personal information, as well as the view shared by de Stadler and Esselaar cited by Heyink (2015), who state that: "It must be recognised that addressing the information security issues will be critical to the achievement of compliance with POPI." Specifically, Condition 7 of the POPI Act (2013), brings to the fore the information security element, in that a selection of security safeguards is required to ensure confidentiality and integrity of personal information.

1.3 Research Problem

As highlighted in the motivation above, Condition 7 of the POPI Act (2013) requires a selection of security safeguards to ensure confidentiality and integrity of personal information. However, the research problem identified is that while the legislative requirement of Condition 7 of the POPI Act (2013) is spelt out in Sections 19, 20, 21 and 22, the requirements are not supported by specific guidance in terms of how the requirements should be satisfied. There is also no specific guidance on the security safeguards, as required in Section 19, to ensure the confidentiality and integrity of specifically electronic personal information. Sikhungo (2016) confirmed this problem and stated that: "POPI does not provide a "tick list" of security requirements to meet. Responsible parties must consider applicable industry security practices and then implement security appropriate security measures for the business." Therefore, in providing a solution to the aforementioned research problem, specifically focused on Condition 7 of the POPI Act (2013) and limited to electronic personal information, this thesis is guided by the following 6 research questions:

- Research question 1 - *To what extent does the privacy legislation of the EU and South Africa address the international 2013 OECD guidelines?*
- Research question 2 - *How can South African institutions, who store, process and transmit electronic personal information achieve and maintain compliance with Condition 7 of the POPI Act (2013), including the security safeguards to be considered to ensure confidentiality and integrity of electronic personal information?*

- Research question 3 - *What is the current level of compliance by South African institutions to the POPI Act (2013) and specifically Condition 7 of the POPI Act (2013)?*
- Research question 4 - *What is the current state of security safeguards within South African institutions to achieve compliance with Condition 7 of the POPI Act (2013), specifically in relation to electronic personal information?*
- Research question 5 - *To what extent is the selection of security safeguards proposed as part of the framework within this thesis valid?*
- Research question 6 - *How can the security safeguards proposed as part of the framework within this thesis be implemented to achieve and maintain confidentiality and integrity of electronic personal information as required by Condition 7 of the POPI Act (2013)?*

1.4 Research Goal, Scope, Limitations and Objectives

The research goal, scope, limitations and objectives are formulated below based on the defined research problem and 6 associated research questions.

1.4.1 Goal

The goal of this research is to provide a solution to the aforementioned research problem by addressing the 6 associated research questions outlined in section 1.3, with a specific focus on Condition 7 of the POPI Act (2013) and limited to electronic personal information.

1.4.2 Scope

Based on the research goal, the scope of this thesis provides a solution that encompasses a framework and model of operation of security safeguards to ensure the confidentiality and integrity of electronic personal information, in order to achieve and maintain compliance with Condition 7 of the POPI Act (2013).

1.4.3 Limitations

This thesis is focused on Condition 7 of the POPI Act (2013) and is limited to electronic personal information. As such, the research survey was specifically targeted at participants from South African institutions who store, process or transmit electronic personal information and who, as a result, are impacted by the POPI Act (2013).

The research is further limited by the South African context, in terms of the implementation of the POPI Act (2013), which at the time of writing this thesis, had still not come into effect, despite being ratified.

Furthermore, this thesis is premised within the information security domain as a result of Condition 7 of the POPI Act (2013). As such, this thesis is not premised in the legal domain and therefore does not in any way aim to encompass an analysis from a legal perspective, for example a legal analysis of the requirements of the POPI Act or EU Data Protection Directive.

1.4.4 Objectives

In analysing the above-mentioned research goal, scope and limitations in conjunction with the research problem and 6 associated research questions, this thesis is guided by the following objectives:

- Exploring the concept and principles of privacy as well as the importance of privacy and providing an overview of the global privacy legislative landscape.
- Providing an overview of South African privacy legislation.
- Analysing the extent to which the privacy legislation of the EU and South Africa addresses the international 2013 OECD guidelines.
- Proposing a framework that includes a selection of security safeguards that may serve as a frame of reference and be used by South African institutions, who store, process and transmit electronic personal information, to ultimately achieve and maintain compliance with Condition 7 of the POPI Act (2013).
- Assessing the level of compliance with the POPI Act (2013) and specifically Condition 7 of the Act, through a research survey aimed at participants from South African institutions.
- Assessing through a research survey aimed at participants from South African institutions the current state of security safeguards within these institutions to

achieve compliance with Condition 7 of the POPI Act (2013), specifically related to electronic personal information.

- Evaluating the applicability and completeness of the selection of security safeguards through a research survey aimed at participants from South African institutions who store, process and transmit electronic personal information, in order to validate the selection of security safeguards of the proposed framework.
- Proposing a model of operation of security safeguards to guide how the selection of security safeguards should be implemented to achieve and maintain the confidentiality and integrity of electronic personal information as required by Condition 7 of the POPI Act (2013).

1.5 RESEARCH METHODOLOGY

The research methodology encompasses a combination of research techniques including a literature review of several sources of information namely, research papers, academic journals, whitepapers, web sites and previous surveys, as well as analysis, modelling and quantitative inferential research, utilising a research survey.

The literature review led to the formulation of the research problem and associated research questions and provided a background in terms of the concept and principles of privacy, the importance of privacy and an overview of the global privacy legislative landscape, including South African privacy legislation. A combination of a literature review and analysis was used to assess the extent to which the privacy legislation of the EU and South Africa addresses the international 2013 OECD guidelines. Modelling was used to propose a framework that includes a selection of security safeguards that may serve as a frame of reference and be used by South African institutions that store, process or transmit electronic personal information, to achieve and maintain compliance with Condition 7 of the POPI Act (2013). The assessment of the level of compliance with the POPI Act (2013) and specifically Condition 7 of the Act was achieved through quantitative inferential research techniques, in the form of a POPI research survey aimed at participants from South African institutions. The POPI research survey was also used to understand the current state of security safeguards within South African institutions and to validate the selection of security safeguards of the proposed framework. Modelling was once again employed to propose the model of operation of security safeguards to guide how the selection of security safeguards should be implemented to achieve and maintain confidentiality and integrity of electronic personal information as required by Condition 7 of the POPI Act (2013).

1.6 Layout

This thesis consists of 10 chapters divided into 7 parts as illustrated in Figure 1.2 below.

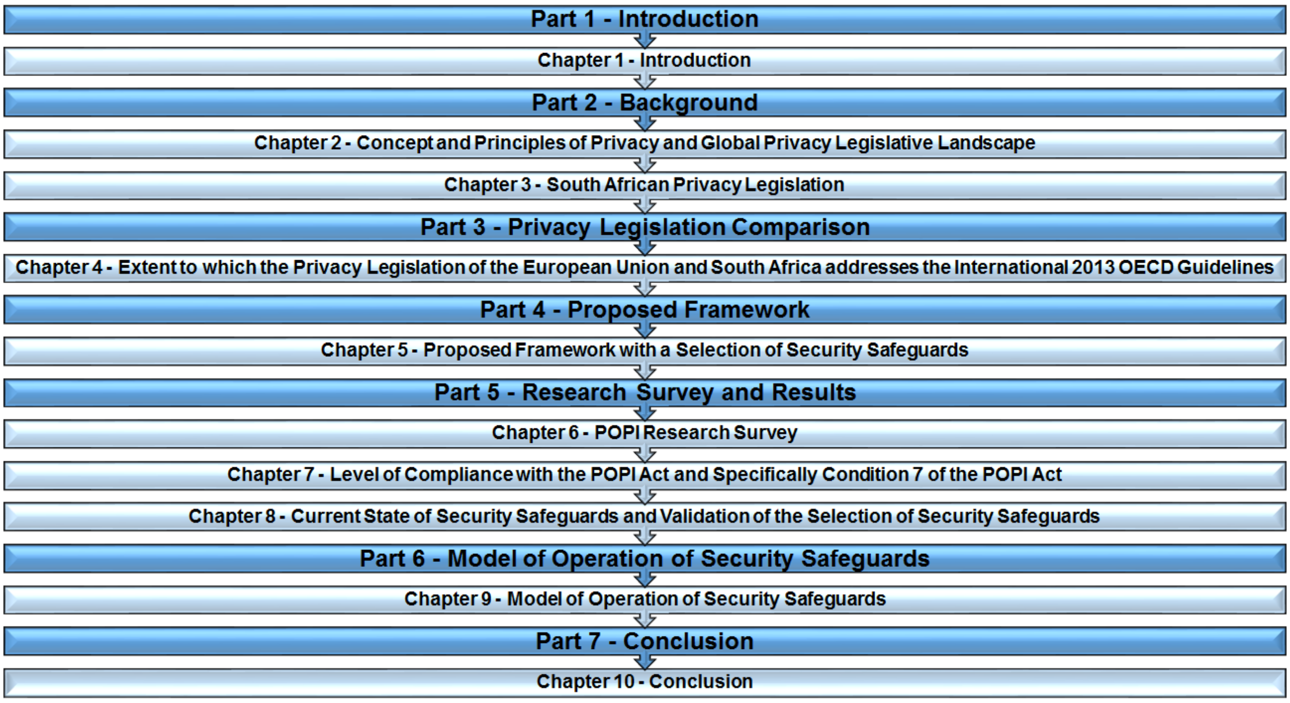

Part 1 - Introduction
Chapter 1 - Introduction
Part 2 - Background
Chapter 2 - Concept and Principles of Privacy and Global Privacy Legislative Landscape
Chapter 3 - South African Privacy Legislation
Part 3 - Privacy Legislation Comparison
Chapter 4 - Extent to which the Privacy Legislation of the European Union and South Africa addresses the International 2013 OECD Guidelines
Part 4 - Proposed Framework
Chapter 5 - Proposed Framework with a Selection of Security Safeguards
Part 5 - Research Survey and Results
Chapter 6 - POPI Research Survey
Chapter 7 - Level of Compliance with the POPI Act and Specifically Condition 7 of the POPI Act
Chapter 8 - Current State of Security Safeguards and Validation of the Selection of Security Safeguards
Part 6 - Model of Operation of Security Safeguards
Chapter 9 - Model of Operation of Security Safeguards
Part 7 - Conclusion
Chapter 10 - Conclusion

Figure 1.2: Layout

Part 1 - Introduction - comprises of Chapter 1, which serves as an introduction to the thesis. This chapter includes the research problem and associated research questions as well as the research goal, scope, limitations, objectives, methodology and layout. In addition, the research publications associated with the thesis in the form of conference research papers and a journal article is provided.

Part 2 - Background - provides a background to the thesis and consists of Chapters 2 and 3. Chapter 2 explores the concept and principles of privacy as well as the importance of privacy in the context of this research and provides an overview of the global privacy legislative landscape. Chapter 3 provides an overview of South African privacy legislation.

Part 3 - Privacy Legislation Comparison - provides a privacy legislation comparison and consists of Chapter 4. This chapter provides the rationale for the privacy legislation comparison followed by the analysis in terms of the extent to which the privacy legislation of the EU and South Africa addresses the international 2013 OECD guidelines. Lastly, this analysis gives rise to a critical evaluation in terms of the similarities and differences associated with the privacy legislation compared within the chapter.

Part 4 - Proposed Framework - comprises of Chapter 5, which proposes a framework that includes a selection of security safeguards that may serve as a frame of reference and be used by South African institutions that store, process and transmit electronic personal information, to achieve and maintain compliance with Condition 7 of the POPI Act (2013). In addition, this chapter provides a critical evaluation in terms of the benefits and limitations associated with the proposed framework.

Part 5 - Research Survey and Results - is made up of Chapter 6, 7 and 8 respectively. Chapter 6 provides an overview of the POPI research survey in terms of the research design, research instrumentation, research group, data analysis approach and the POPI research survey results in terms of demographics as it relates to the participants' institutions' sector (public versus private), industry sector and institution size. Chapter 7 provides the level of compliance with the POPI Act (2013) and specifically Condition 7 of the Act as well as the financial value associated with electronic personal information and the potential impact of a data breach of electronic personal information. Furthermore, Chapter 8 focuses on the current state of security safeguards within South African institutions and validates the selection of security safeguards of the proposed framework from Chapter 5 through the POPI research survey results. Lastly, a critical evaluation in terms of key findings and recommendations based on the analysis of the POPI research survey results is provided in Chapter 7 and 8 respectively.

Part 6 - Model of Operation of Security Safeguards - consists of Chapter 9, which proposes a model of operation of security safeguards to guide one on how the selection of security safeguards should be implemented to achieve and maintain confidentiality and integrity of electronic personal information as required by Condition 7 of the POPI Act (2013). In addition, this chapter provides the benefits and limitations associated with the model of operation of security safeguards as part of a critical evaluation.

Part 7 - Conclusion - comprises of Chapter 10 devoted to concluding the thesis. The final chapter assesses the extent to which the research problem and associated research questions have been addressed by the thesis. In addition, the final chapter provides the research contribution associated with the thesis as well as highlights potential areas of future research.

Finally, the appendices associated with this thesis as well as a bibliography of research consulted during the formulation of this thesis is provided after the last chapter.

1.7 Research Publications

During the process of formulating this thesis, research publications were produced in the form of peer-reviewed conference research papers and a journal article was formulated to be submitted to a peer-reviewed journal for consideration and publication.

The research publications in the form of published peer-reviewed conference research papers are provided in Appendix F and a summary is provided in Table 1.1 below, in chronological order based on the date that they were presented at the respective conferences.

Table 1.1: Research Publications

Conference research paper title	Conference	Date and location	Acceptance rate
A Framework of Security Safeguards for	10th International Conference on	24 to 25 March 2015.	Acceptance Rate: 47%.

Conference research paper title	**Conference**	**Date and location**	**Acceptance rate**
Confidentiality and Integrity of Electronic Personal Information.	Cyber Warfare and Security (ICCWS) 2015.	Kruger National Park, South Africa.	Received the Joint Award for the Best Conference Paper presented at ICCWS 2015.
The Extent to which Privacy Legislation of the European Union and South Africa addresses the 2013 OECD Guidelines.	African Cyber Citizenship Conference (ACCC) 2015.	2 to 3 November 2015 Port Elizabeth, South Africa.	Acceptance Rate: 39%
Understanding the Level of Compliance by South African Institutions to the POPI Act (2013).	South African Institute of Computer Scientists and Information Technologists (SAICSIT) 2016.	26 to 28 September 2016. Johannesburg, South Africa.	Acceptance Rate: 39%.
The Current State of Security Safeguards within South African Institutions to achieve Compliance to Condition 7 of the POPI Act (2013).	African Cyber Citizenship Conference (ACCC) 2016.	31 October 2016 to 1 November 2016. Port Elizabeth, South Africa.	Acceptance Rate: 52%

At the time of concluding and submitting this thesis for examination, a journal article entitled: *A Model of Operation for Electronic Personal Information to Achieve and Maintain*

Compliance to Condition 7 of the POPI Act was formulated and submitted to a peer-reviewed journal for consideration and publication.

1.8 Conclusion

Part 1 (Introduction) of this thesis was concluded in terms of Chapter 1, which served as an introduction to the thesis and as a result of a literature review, the research problem and associated research questions were defined. In addition, the research goal, scope, limitations, objectives, methodology and layout were provided. Lastly, the research publications associated with the thesis in the form of conference papers and a journal article were provided.

As such, Table 1.2 below demonstrates the relationship between the research questions defined based on the research problem and the layout of the thesis together with the research publications produced as a result of this thesis. For example, the research question 2, "*How can South African institutions, who store, process and transmit electronic personal information achieve and maintain compliance with Condition 7 of the POPI Act, including the security safeguards to be considered to ensure confidentiality and integrity of electronic personal information?*" is addressed by Chapter 5 within Part 4, of the thesis, "*Proposed Framework with a Selection of Security Safeguards*", which is associated with a peer-reviewed conference research paper titled, "*A Framework of Security Safeguards for Confidentiality and Integrity of Electronic Personal Information*", which was published in the conference proceedings of the 10th International Conference on Cyber Warfare and Security in 2015.

Table 1.2: Research Questions, Layout and Research Publications

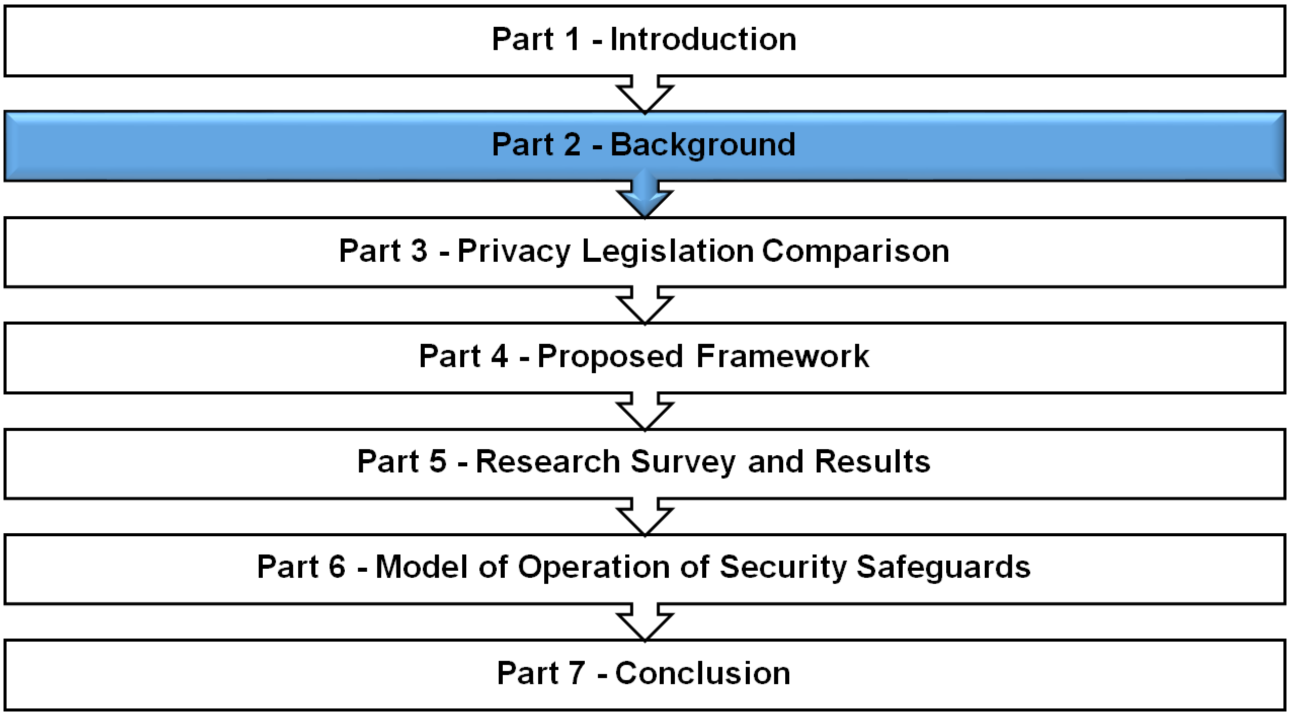
Research question	**Layout**	**Research publications**
Research question 1 - *To what extent does the privacy legislation of the EU and South Africa address the international 2013 OECD guidelines?*	Part 2 - Chapter 4: Extent to which the Privacy Legislation of the EU and South Africa addresses the	Conference paper published and presented - ACCC 2015: *The Extent to which Privacy Legislation of the EU and*

Research question	Layout	Research publications
	international 2013 OECD Guidelines.	*South Africa addresses the 2013 OECD Guidelines.*
Research question 2 - *How can South African institutions, that store, process and transmit electronic personal information achieve and maintain compliance with Condition 7 of the POPI Act (2013), including the security safeguards to be considered to ensure the confidentiality and integrity of electronic personal information?*	Part 3 - Chapter 5: Proposed Framework with a Selection of Security Safeguards.	Conference paper published and presented - ICCWS 2015: *A Framework of Security Safeguards for Confidentiality and Integrity of Electronic Personal Information.*
Research question 3 - *What is the current level of compliance by South African institutions to the POPI Act (2013) and specifically Condition 7 of the Act?*	Part 4 - Chapter 7: Level of Compliance with the POPI Act and specifically Condition 7 of the POPI Act.	Conference paper published and presented - SAICSIT 2016: *Understanding the Level of Compliance by South African Institutions to the POPI Act (2013).*
Research question 4 - *What is the current state of security safeguards within South African institutions to achieve compliance with Condition 7 of the POPI Act (2013), specifically in relation to electronic personal information?*	Part 4 - Chapter 8: Current State of Security Safeguards and Validation of the Selection of Security Safeguards.	Conference paper published and presented - ACCC 2016: *The Current State of Security Safeguards within South African Institutions to Achieve Compliance to Condition 7 of the POPI Act.*
Research question 5 - *To what extent is the selection of security safeguards proposed as part of the*		

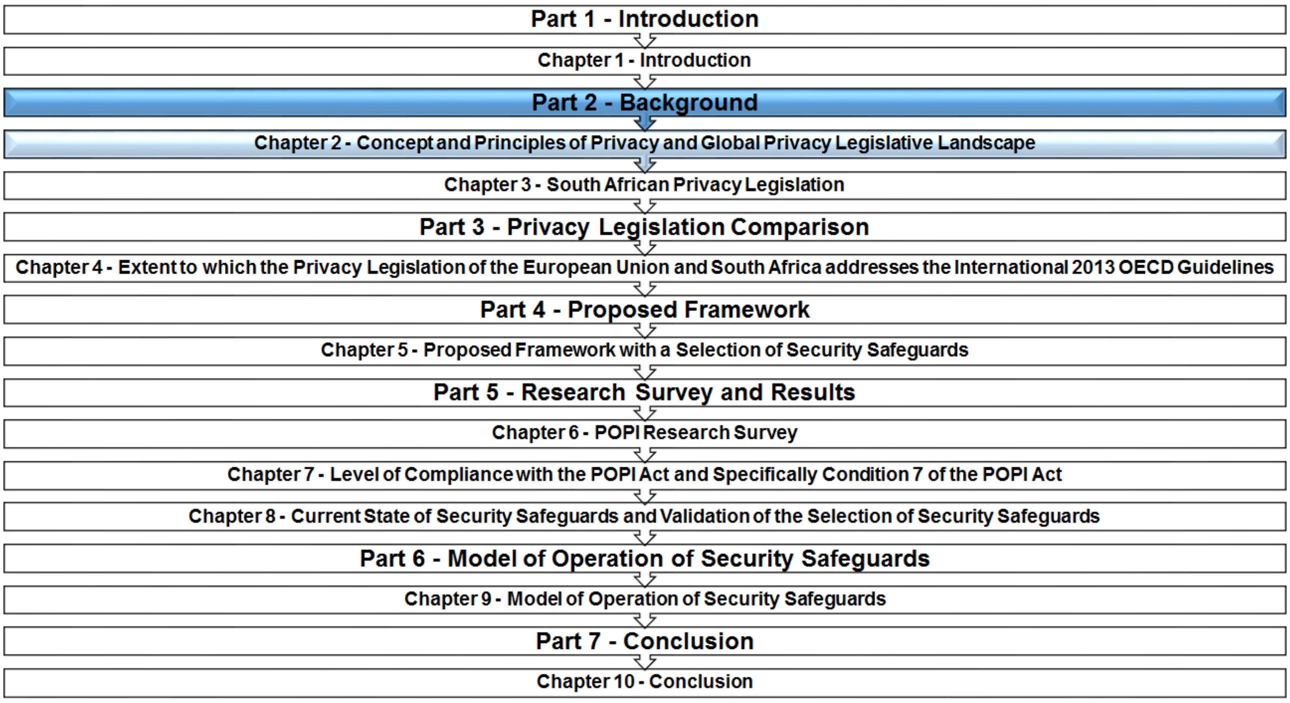
Research question	Layout	Research publications
framework within this thesis valid?		
Research question 6 - *How can the security safeguards proposed as part of the framework within this thesis be implemented to achieve and maintain confidentiality and integrity of electronic personal information as required by Condition 7 of the POPI Act (2013)?*	Part 5 - Chapter 9: Model of Operation of Security Safeguards.	Journal article formulated in 2017 to be submitted to a peer-reviewed journal for consideration and publication: *A Model of Operation for Electronic Personal Information to Achieve and Maintain Compliance to Condition 7 of the POPI Act*.

Part 2 (Background) of this thesis follows this chapter and serves to provide a background to the thesis in Chapter 2 and 3 respectively. Chapter 2 explores the concept and principles of privacy as well as the importance of privacy and provides an overview of the global privacy legislative landscape. Chapter 3 provides an overview of South African privacy legislation.

PART 2 - BACKGROUND


Part 1 - Introduction
Part 2 - Background
Part 3 - Privacy Legislation Comparison
Part 4 - Proposed Framework
Part 5 - Research Survey and Results
Part 6 - Model of Operation of Security Safeguards
Part 7 - Conclusion

CHAPTER 2 - CONCEPT AND PRINCIPLES OF PRIVACY AND GLOBAL PRIVACY LEGISLATIVE LANDSCAPE


Part 1 - Introduction
Chapter 1 - Introduction
Part 2 - Background
Chapter 2 - Concept and Principles of Privacy and Global Privacy Legislative Landscape
Chapter 3 - South African Privacy Legislation
Part 3 - Privacy Legislation Comparison
Chapter 4 - Extent to which the Privacy Legislation of the European Union and South Africa addresses the International 2013 OECD Guidelines
Part 4 - Proposed Framework
Chapter 5 - Proposed Framework with a Selection of Security Safeguards
Part 5 - Research Survey and Results
Chapter 6 - POPI Research Survey
Chapter 7 - Level of Compliance with the POPI Act and Specifically Condition 7 of the POPI Act
Chapter 8 - Current State of Security Safeguards and Validation of the Selection of Security Safeguards
Part 6 - Model of Operation of Security Safeguards
Chapter 9 - Model of Operation of Security Safeguards
Part 7 - Conclusion
Chapter 10 - Conclusion

2.1 INTRODUCTION

Chapter 1 provided an introduction to the thesis. This thesis is underpinned within the privacy domain specifically in the context of privacy legislation to ultimately protect personal information. As such, this chapter unpacks the concept and principles of privacy as well as the importance of privacy and also provides an overview of the global privacy legislative landscape.

2.2 PRIVACY CONCEPT

The concept of privacy dates back to as early as the era of Greek philosophers such as Socrates, in that his writings differentiated between ‘public’ and ‘private’, ‘inner’ and ‘outer’ as well as ‘society’ and ‘solitude’ (Holvast, 2009). According to Holvast (2009), the concept has evolved from a period of understanding the importance of privacy to a period of taking measures in the form of privacy regulations and more recently, to a deep understanding of the critical role played by information in combating fraud, criminality and terrorism.

Despite the evolution of privacy, Solove (2006 and 2008) characterised the concept as suffering from an “embarrassment of meanings” and argues that it is a concept in disarray as: “It is a sweeping concept, encompassing (among other things) freedom of thought, control over one’s body, solitude in one’s home, control over personal information, freedom from surveillance, protection of one’s reputation, and protection from searches and interrogations.” As such, Solove (2002) demystified the concept of privacy and stated that privacy entails the right to be left alone, providing limited self-access, maintaining secrecy, controlling personal information, the protection of personhood in terms of personality, individuality and dignity as well as intimacy by controlling access to aspects of life and intimate relationships. Similarly, the philosophical dimensions of Schoeman’s (1984) privacy study associated the concept of privacy with claim, entitlement, right, the degree of control, access and visibility to personal information and intimacy. In addition, Gormley (1992) explored the concept of privacy and a similar association is made in terms of autonomy, personhood, and the ability to regulate personal information as well as secrecy, anonymity and solitude also affirmed by Gavison (2012). Furthermore, according to Privacy International (2017) the concept of privacy enables the creation and management of boundaries to ultimately serve as a form of protection in terms of controlling who has access to an individual's body, place, possessions, communication and information. The concept of privacy in a South African context is provided from a legal perspective in terms of the definition by Neethling (2005), which is accepted in case law - *National Media Ltd v Jooste*. This definition by Neethling (2005) states that: "privacy can be described as a condition of human life characterized by seclusion from the public and publicity. This condition embraces all those personal facts which the person concerned has himself determined to be excluded from the knowledge of outsiders and in respect of which he has the will that they be kept private". As such Roos (2007) argues, based on definition of privacy provided by Neethling (2005), that privacy allows an individual to have control in terms of either sharing or restricting information, such as personal information.

A common theme associated with the concept of privacy as highlighted by the aforementioned researchers is the ability to control. This theme is affirmed by Galvez Cruz (2008) and Reddy (2012) who also explored the concept of privacy, as part of their respective research theses, in order to adopt a formal definition of privacy. According to Galvez Cruz (2008) privacy allows a person to be in control of disclosure, personal information and boundaries. Similarly, Reddy (2012) stated that: "privacy is the right of individuals to control both information about themselves and their boundaries during interactions with others".

A further clarification of the concept of privacy is achieved by understanding the context in which privacy is applied i.e. what an individual is able to control, therefore giving rise to the different types of privacy. As a result, Clarke (1997) who according to Finn et al. (2013) was the first to formulate the types of privacy in logical and structured manner as illustrated in Table 2.1 below.

Table 2.1: Types of Privacy

Source: Adapted from Clarke (1997)

Privacy type	**Definition**
Bodily Privacy	Addresses the integrity associated with a person's

Privacy type	**Definition**
	body, such as blood transfusion without consent.
Behaviour Privacy	Addresses all behavioural aspects in both public and private locations and is particularly focused on sexual preferences and habits, political activities and religious practices.
Personal Communication Privacy	Addresses the ability for individuals to utilise various forms of media to communicate with other individuals, without the prevailing communication being subjected to monitoring by individuals or institutions.
Personal Data Privacy	Addresses the ability of individuals to control the access and use of personal data by other individuals or institutions.

Holvast (2009), identified bodily and personal data privacy types same as was identified by Clarke (1997) with the exception of the territorial privacy type. Territorial privacy addresses who has access to a person's belongings such as a home or car (Holvast, 2009). Similar to Clarke (1997) and Holvast (2009), Banisar and Davies (Unknown) identified bodily, personal communication, personal data (information) and territorial privacy types. However, more recently in 2013, Finn et al. (2013) proposed an expansion to the different privacy types by Clarke (1997), from 4 to 7 privacy types, due to the advances in technology such as whole body imaging scanners, unmanned aerial vehicles, human enhancement technologies and second-generation biometrics. As a result, based on these advances in technology, Finn et al. (2013) expanded upon the bodily, behaviour, personal communication and personal data privacy types by Clarke (1997) and proposed new privacy types related to association, thoughts and feelings as well as location and space. Association privacy addresses the ability of an individual to associate with any individual or group free from being monitored (Finn et al., 2013). Thoughts and feelings privacy addresses the ability of an individual not to share or reveal their thoughts and feelings (Finn et al., 2013). Location and space privacy allows individuals the ability to freely move around without being identified, tracked or monitored (Finn et al., 2013).

In 2013, Clarke (2013) expanded upon the types of privacy to include personal experience privacy that addresses the need to protect an individual's personal experience from exploitation. For example, the locations of individuals may be tracked and analysed to ascertain who is meeting with who and the frequency thereof. This privacy type proposed by Clarke (2013) was the same as the location and space privacy type proposed by Finn et al. (2013).

As a result of understanding the concept of privacy and the different types of privacy, Moore's (2008) definition of the concept of privacy which focuses on controlling the use and access of place, location and in particular personal information is adopted as the most appropriate for this thesis. This definition of the concept of privacy by Moore (2008) adequately addresses the fundamentals of privacy in a non-complicated fashion by focusing on the theme of control in the appropriate context which in this instance is related to the personal data (information) privacy type given the focus area of this thesis in terms of the related privacy legislation to ultimately achieve the protection of personal information or personal data (information) privacy as described by Clarke (1997), Holvast (2009), Banisar and Davies (Unknown), Finn et al. (2013).

Having formally adopted a definition of privacy for the purpose of this thesis, it is important to also explore the privacy principles.

2.3 PRIVACY PRINCIPLES

In 1980, the Organisation for Economic Co-operation and Development (OECD), which is a forum in which governments collaborate to share experiences and solve problems in order to improve the economic and social well-being of people around the world (OECD, 2015), adopted international guidelines on trans-border data flows and the protection of privacy (OECD, 1980).

At that stage, the major drivers for these guidelines were the threats associated with privacy due to the ever increasing use of personal information and the impact restrictions on the flow of information had on the global economy (OECD, 2011a). As a result, the guidelines included 8 privacy principles as illustrated in Table 2.2 to govern the preservation of privacy and trans-border flow of personal information (OECD, 1980). These guidelines were recommended to OECD member states to be applied to all personal information by both public and private institutions (OECD, 1980 and Kirby, 2011).

Table 2.2: OECD Privacy Principles Adopted in 1980

Source: Adapted from OECD (1980)

Number	Privacy principle	Privacy principle description
1	Collection limitation principle	There should be limits to the collection of personal information and it should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
2	Data quality principle	Personal information should be relevant to the purposes for which they are to be used and to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.
3	Purpose specification principle	The purposes for which personal information is collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
4	Use limitation principle	Personal information should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with the purpose specification principle, except: a) With the consent of the data subject. b) By the authority of law.

Number	Privacy principle	Privacy principle description
5	Security safeguards principle	Personal information should be protected by reasonable security safeguards against risks such as loss or unauthorised access, destruction, use, modification or disclosure of data.
6	Openness principle	There should be a general policy of openness about the developments, practices and policies with respect to personal information. Means should be readily available of establishing the existence and nature of personal information, and the main purposes of their use, as well as the identity and usual residence of the data controller.
7	Individual participation principle	An individual should have the right: a) To obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him. b) To be communicated to him, data relating to him within a reasonable time; at a charge, if any that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him. c) To be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial. d) To challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended.
8	Accountability principle	A data controller should be accountable for complying with measures which give effect to

Number	Privacy principle	Privacy principle description
		the seven other privacy principles stated above.

The 1980 international guidelines on trans-border data flows and the protection of privacy were revised by the OECD in 2013. Major drivers for the revision of the 1980 guidelines were due to increased globalisation of the world economy, growing economic importance of data processing, ubiquity of data transfers over the Internet, greater direct involvement in trans-border data flows, changing role of geography, growing risk to the privacy of individuals (Kuner, 2011). These drivers were further supported by an evolving privacy landscape that presented an ever increasing volume of personal information being collected, used and stored, the range of analytics enabled by personal information, providing insights into individual and group trends, movements, interests, and activities, the value of the societal and economic benefits enabled by new technologies and responsible uses of personal information (OECD, 2011b). In addition, the extent of threats to privacy, the number and variety of actors capable of either putting privacy at risk or protecting privacy, the frequency and complexity of interactions involving personal information that individuals are expected to understand and negotiate as well as the global availability of personal information, supported by communications networks and platforms that permit continuous, multipoint data flows all served to reinforce the key drivers associated with the evolving privacy landscape (OECD, 2011b).

The 8 privacy principles (collection, data quality, purpose specification, use limitation, security safeguards, openness, individual participation and accountability) prescribed within the guidelines in 1980 by the OECD remained unchanged in the 2013 revision of the guidelines (Kuschewsky, 2014). However, the 2013 guidelines placed greater focus on implementing accountability, the basic principles of international application in terms of free flow and legitimate restrictions, national implementation as well as international co-operation and interoperability (OECD, 2013).

In terms of implementing accountability an adequate privacy management programme has to be defined and implemented and be subject to review from a privacy enforcement authority as well as providing notice to the privacy enforcement authority in the event of a breach of personal information (OECD, 2013).

With regards to the basic principles of international application in terms of free flow and legitimate restrictions, an organisation (the data controller) remains accountable for the personal information irrespective of the location of the data. Tans-border data flows should not be restrictive if other country applies the guidelines and if restrictions are required, the risk should be assessed in relation to the privacy principles (OECD, 2013).

National implementation addresses the privacy strategies and laws that should be defined and implemented by countries as well as key considerations such as sanctions, unfair discrimination which should be taken into account during implementation (OECD, 2013).

International co-operation and interoperability deals with the cross border privacy law enforcement, international arrangements that promote interoperability among privacy frameworks, sharing of information in relation to compliance with the guidelines (OECD, 2013).

2.4 IMPORTANCE OF PRIVACY

The drivers for the development of the OECD international guidelines in 1980 which included the 8 privacy principles and the most recent revision of the OECD international guidelines in 2013 clearly demonstrate the importance of privacy. Prior to the OECD international guidelines the importance of privacy as a basic human right was reflected within Article 12 of Universal Declaration of Human Rights by the United Nations (1948) and Article 17 of the International Covenant on Civil and Political Rights by the United Nations (1966).

According to Clarke (2006), privacy is important from a social, economic, political and psychological perspective. Socially individuals, need to be free to interact, associate and behave without being subject to surveillance (Clarke, 2006). From an economic perspective individuals require ongoing freedom to innovate in order to remain competitive and contribute to a sustainable economy (Clarke, 2006). Politically individuals need to be afforded freedom to think, argue and act in order to ensure a healthy democracy (Clarke, 2006). Lastly, from a psychological perspective, individuals require their private space and the ability to control the use and access thereof (Clarke, 2006). In a similar fashion, Holvast (2009) highlights the importance of privacy in relation to modern life by expressing the need for personal autonomy as privacy is the basis for the development of individuality as well as the need for emotional release due to physical and psychological health demands of life. In addition, the importance of privacy, as it relates to decision making and self-evaluation by individuals, as well as the need to ensure limited and protected communication, is also highlighted by Holvast (2009). However, Holvast (2009) differs from Clarke (2006) by adding the technology dimension, and as a result, highlights the importance of privacy in present technology, such as video surveillance, biometric identification, genetic data, identity theft, data warehousing and data mining, chips or smartcards, global positioning system, Internet, key loggers, radio frequency identification, wireless networking and the Internet of Things (IoT) as well as smart homes and future technology such as neurolinguistics, memetics, ambient and grid technology.

2.5 GLOBAL PRIVACY LEGISLATIVE LANDSCAPE

Privacy is therefore important in the social, economic, political and technological contexts. As a result, an invasion or a violation of privacy may take place within the aforementioned contexts, ultimately impacting an individual’s ability to control the use and access to place, location and personal information. As such, Greenleaf (2013) states that data privacy laws serve as the legal instrument most capable of preserving privacy. Therefore, armed with an understanding of the privacy concept and principles as well as the importance of privacy, globally many countries commenced with the development and in some cases have fully implemented privacy legislation in the form of data protection laws and regulations, which specifically focus on the protection of personal information.

The European Union (EU) has adopted the Data Protection Directive (also known as Directive 95/46/EC) of 1995 to protect personal information of individuals within EU member states (European Parliament, 1995). The United States of America (USA) responded to meet the requirements of the Data Protection Directive (1995), specifically relating to the adequacy standard, by introducing the Safe Harbor Act of 2000 designed to allow for the transfer of personal information between EU member states and the USA (Steinke, 2002). Furthermore, in the USA the Privacy Act of 1974 (United States Department of Justice, 2015) is in place to regulate the information practices of the public sector, however there is no comprehensive privacy protection law in place for the private sector, instead various Amendments as part of the Constitution (1789) and federal laws are in place. The First Amendment of the Constitution of the USA (1791) protects the freedom of expression, religion, and assembly. The Fourth Amendment of the Constitution of the USA (1791) prohibits unreasonable search and seizure. The Fourteenth Amendment (1795) guarantees due process and non-disclosure of personal information. Federal laws, as cited by Holvast (2009), also address the protection of personal information as it relates to financial records, credit reports, educational records, telephone records, video rentals and cable television.

Canada has the Personal Information Protection and Electronic Document Act (PIPEDA) of 2000 in place to govern how organisations collect, use and disclose personal information (Government of Canada, 2014). Similarly, protection of personal information legislation has been adopted by several countries such as Argentina in the form of the Personal Data Protection Act (Government of Argentina, 2000), Australia in terms of the Privacy Act (Government of Australia, 1988), Japan in the form of the Personal Information Protection Law (Government of Japan, 2003) and New Zealand in terms of the Privacy Act (Government of New Zealand, 1993).

The global privacy legislative landscape is eloquently captured by the *Data Protection Laws of the World Handbook* (DLA Piper, 2016), in that it provides a comprehensive listing and current status of data protection laws and regulations for several countries on an annual basis. The latest edition of the *Data Protection Laws of the World Handbook* (DLA Piper, 2016) included 89 countries such as Angola, Brazil, Cayman, China Islands, Denmark, Estonia, France, Hong Kong, Iceland, India, Netherlands, Lithuania, Nigeria, Philippines, Russia, Singapore, South Korea, Thailand, and the United Arab Emirates.

In addition, Figure 2.1 below illustrates on a global scale as at February 2017 the extent of data protection regulation and enforcement.

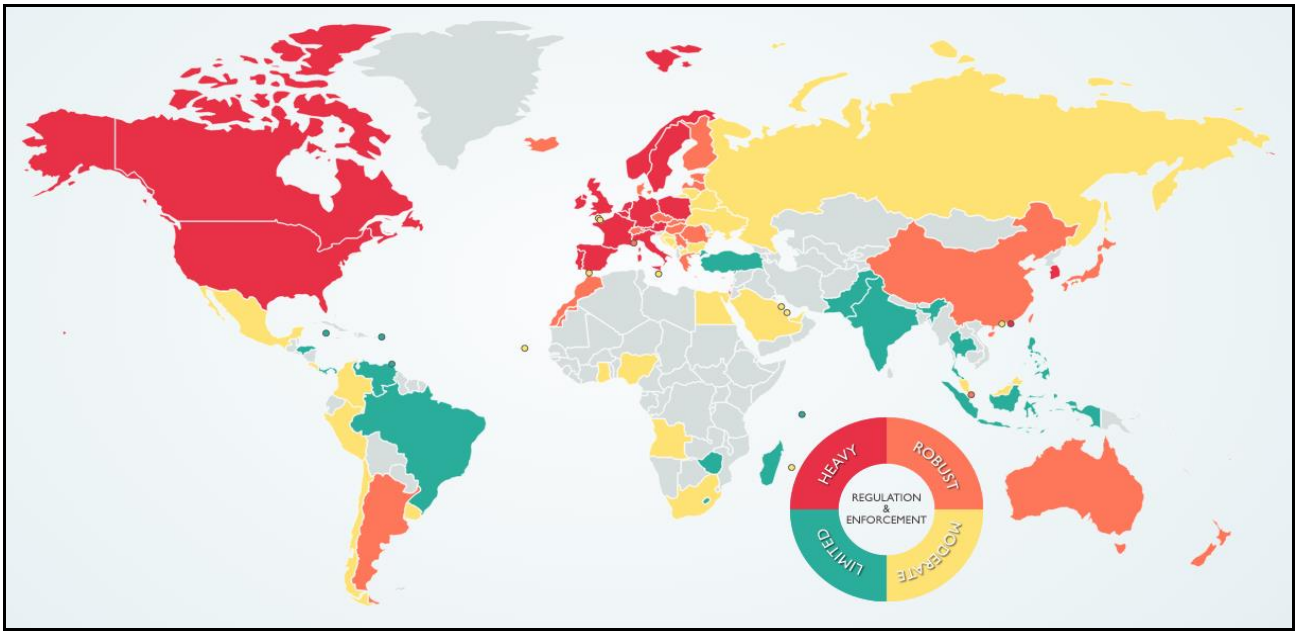


Figure 2.1: Extent of Data Protection Regulation and Enforcement - February 2017

Source: DLA Piper (2017)

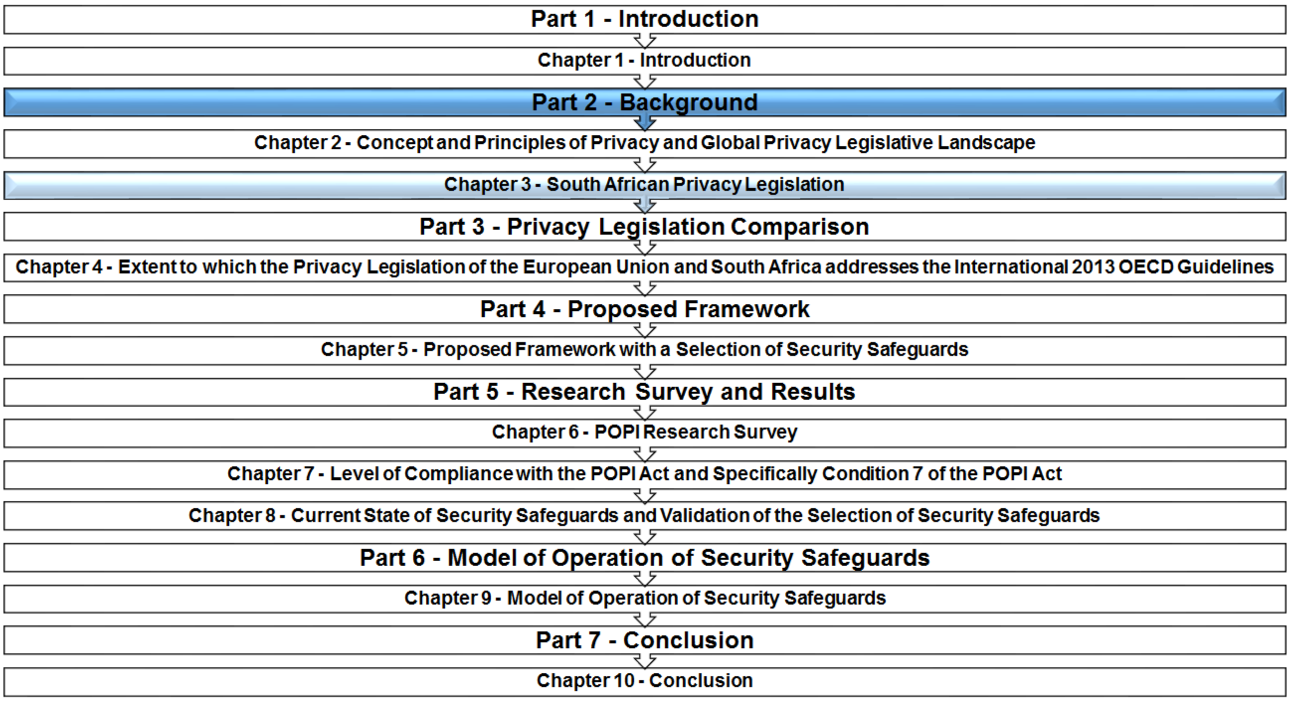
There is a robust degree of data protection regulation and enforcement in Argentina, Australia and China compared to countries such as Belgium, Canada, France, Germany, Italy, Norway, Spain, Sweden, United Kingdom and the United States of America where there is a high degree of data protection regulation and enforcement (DLA Piper, 2017). Countries such as Angola, Columbia, Egypt, Nigeria, Russia, Saudi Arabia and South Africa have a moderate degree of data protection regulation and enforcement compared to countries such as Brazil, India, Indonesia, Pakistan, Turkey and Zimbabwe who have a low degree of data protection regulation and enforcement (DLA Piper, 2017).

2.6 CONCLUSION

This chapter in terms of Part 2 (Background) of this thesis explored the concept and principles of privacy as well as the importance of privacy and provided an overview of the global privacy legislative landscape.

The next chapter which also forms part of the background of this thesis explores the South African response in relation to privacy legislation.

CHAPTER 3 - SOUTH AFRICAN PRIVACY LEGISLATION



Part 1 - Introduction

Chapter 1 - Introduction

Part 2 - Background

Chapter 2 - Concept and Principles of Privacy and Global Privacy Legislative Landscape

Chapter 3 - South African Privacy Legislation

Part 3 - Privacy Legislation Comparison

Chapter 4 - Extent to which the Privacy Legislation of the European Union and South Africa addresses the International 2013 OECD Guidelines

Part 4 - Proposed Framework

Chapter 5 - Proposed Framework with a Selection of Security Safeguards

Part 5 - Research Survey and Results

Chapter 6 - POPI Research Survey

Chapter 7 - Level of Compliance with the POPI Act and Specifically Condition 7 of the POPI Act

Chapter 8 - Current State of Security Safeguards and Validation of the Selection of Security Safeguards

Part 6 - Model of Operation of Security Safeguards

Chapter 9 - Model of Operation of Security Safeguards

Part 7 - Conclusion

Chapter 10 - Conclusion

3.1 INTRODUCTION

Chapter 2 provided an understanding of the global privacy legislative landscape in addition to the concept and principles of privacy as well as the importance of privacy. This chapter provides an overview of the South African response to privacy legislation which has the taken the form of the Protection of Personal Information (POPI) Act (Act 4 of 2013). The discourse in this chapter includes the need for privacy legislation in South Africa, the journey from POPI Bill to Act, the purpose of the Act, personal information defined in terms of the Act, applicability, accountability and exclusions of the Act, the requirements of the Act and specifically Condition 7, the establishment of an Information Regulator and the commencement date of the Act. This will be followed by the risks and opportunities associated with the POPI Act (2013).

3.2 THE NEED FOR PRIVACY LEGISLATION IN SOUTH AFRICA

The information age we live in is continually the subject of data breaches involving personal information (Anandarajan et al., 2013). South Africa is not immune to data breaches of personal information. As such during 2016, as mentioned in Chapter 1 of this thesis, Government Communication and Information Services (GCIS) (Vermeulen, 2016a), the Department of Water Affairs (Vermeulen, 2016b), Armscor (MyBroadBand, 2016a), the Ethekwini Municipality (MyBroadBand, 2016b) and MTN (MyBroadBand, 2016c) all suffered data breaches of personal information which became public knowledge. Furthermore, South Africa faces a growing problem in terms of the extensive amount of personal information being disclosed online through electronic documents available on web sites (Grobler et al., 2014). As a result, between 12 November 2013 and 30 May 2014, in an investigation by Grobler et al. (2014), a number of personal information records, as listed in Table 3.1 on the next page, were disclosed by 293 out of 2714 unique South African domains (co.za) evaluated during the aforementioned period.

Table 3.1: Number of Personal Information Records Disclosed in South Africa

Source: Adapted from Grobler et al. (2014)

Personal information record type	Number of personal information records disclosed in South Africa from 12 November 2013 to 30 May 2014
Identity number	892 811
Landline number	852 713
Cellphone number	1 214 516
Email address	407 307
Credit card number	78 037
Addresses	537 141

To further compound the problem, the disclosure of personal information records as a result of a data breach, negligence or accident by South African institutions is often associated with a lack of transparency and cover-ups (Floor, 2015). This is due to the lack of privacy legislation compelling South African institutions to notify the public in the event of an unauthorised disclosure of personal information records as a result of a data breach, negligence or accident (Alfreds, 2016).

As such, there was a great need for privacy legislation in South Africa required to provide the legal platform capable of protecting personal information for enforcing a greater deal of accountability and responsibility when dealing with personal information and most importantly, to ensure transparency by South African institutions in the event of a data breach, negligence or accident associated with personal information. In addition, the concept of privacy is enshrined in Section 14 of the South African Constitution (1996), which is the supreme law of the land that affords every individual a right to privacy. As such, Neethling et al. (2005) argues this right to privacy afforded to every individual in the Constitution further enhances the need for privacy legislation to be enacted in South Africa to protect personal information.

Furthermore, under South African common law, privacy is recognised and protected in relation to an individual in terms of personality interest - physical liberty, good name, dignity, feelings, privacy and identity (Roos, 2007). However, according to Roos (2016), the common law principles present a shortcoming in terms of effectively protecting privacy as an individual does not know when personal information is collected, if it is correct and who has access to this information. Neethling et al. (2005) affirms this common law shortcoming associated with personal information. Due to the common law shortcoming to effectively protect privacy both Roos (2016) and Neethling (2016) identify that there is an urgent need for privacy legislation in South Africa to protect personal information.

Therefore, privacy legislation in South Africa to protect personal information is the natural progression required to enforce the preservation of the right to privacy afforded to every individual and address the shortcoming presented by common law to effectively protect privacy. Furthermore, according to Roos (2006 and 2007) privacy legislation is critical from an international perspective if South Africa aims to remain part of the international information community and global economy.

3.3 JOURNEY FROM POPI BILL TO ACT

Privacy legislation to address the protection of personal information in South Africa was first published for comment in 2005 (Stein, 2012) in the form of the POPI Bill (2009). After being made available for public scrutiny and comment as well as lengthy and detailed deliberations and numerous reviews, the POPI Bill (2009) was subjected to the final process of becoming an Act. This process involved tabling the POPI Bill (2009) in Parliament for comment by the Parliamentary Portfolio Committee on Justice and thereafter it was submitted for approval to the National Council of Provinces, followed by the National Assembly. Finally, after an extensive journey, the POPI Bill was enacted and signed into law by the President of the Republic of South Africa on 26 November 2013 as the POPI Act (2013) and published in the Government Gazette. However, the commencement date of the POPI Act (2013) is still to be announced.

3.4 PURPOSE OF THE POPI ACT

The purpose of the POPI Act (2013), as outlined in Section 2, is to: “promote the protection of personal information processed by public and private bodies; to introduce certain conditions so as to establish minimum requirements for the processing of personal information; to provide for the establishment of an Information Regulator to exercise certain powers and to perform certain duties and functions in terms of this Act and the Promotion of Access to Information Act, 2000; to provide for the issuing of codes of conduct; to provide for the rights of persons regarding unsolicited electronic communications and automated decision making; to regulate the flow of personal information across the borders of the Republic; and to provide for matters connected therewith."

In essence, the POPI Act (2013) aims to ensure the right to privacy by offering individuals: "a right to protection against the unlawful collection, retention, dissemination and use of personal information."

3.5 PERSONAL INFORMATION

Since personal information is mentioned throughout this thesis, a common understanding of personal information is critical. As a result, the definition of personal information as specified by the POPI Act (2013) below, is deemed to be the most suitable, given that personal information will be studied in the context of requirements specified within the POPI Act (2013) itself.

Any information relating to an identifiable, living and natural individual is referred to as personal information (Organisation for Economic Co-operation and Development (OECD), 2013). This definition of personal information by the OECD (2013) is extended upon in Section 1 of the POPI Act (2013), which defines personal information as: "information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to:

(a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;

(b) information relating to the education or the medical, financial, criminal or employment history of the person;

(c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;

(d) the biometric information of the person;

(e) the personal opinions, views or preferences of the person;

(f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;

(g) the views or opinions of another individual about the person; and

(h) the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person."

Personal information stored, processed or transmitted may exist in electronic format (within information systems and their corresponding databases) or non-electronic format (hard copy or paper based outside information systems).

3.6 APPLICABILITY, ACCOUNTABILITY AND EXCLUSIONS OF THE POPI ACT

The protection of personal information as specified by the POPI Act (2013) is applicable to public and private institutions in South Africa. A public institution in terms of the POPI Act (2013) is referred to as a "public body" and defined as: "(a) any department of state or administration in the national or provincial sphere of government or any municipality in the local sphere of government; or (b) any other functionary or institution when - (i) exercising a power or performing a duty in terms of the Constitution or a provincial constitution; or (ii) exercising a public power or performing a public function in terms of any legislation". A private institution in terms of the POPI Act (2013) is referred to as a "private body" and defined as: "(a) a natural person who carries or has carried on any trade, business or profession, but only in such capacity; (b) a partnership which carries or has carried on any trade, business or profession; or (c) any former or existing juristic person, but excludes a public body".

Therefore, public and private institutions that collect, store, process or disseminate personal information as part of their business activities are impacted by the Act (De Bruyn, 2014). The coverage of the POPI Act (2013) in terms of both public and private institutions is aligned with Greenleaf's (2013) view that privacy legislation should cover most of a country's private and public sectors and not only be focused on a few sub-sectors, like "credit reporting" or "health".

Furthermore, accountability for compliance with the POPI Act (2013) rests with the responsible party defined within the Act as: "a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information". According to Monty (2015), the responsible party must be resident in South Africa or the processing must take place in the country, subject to certain exclusions and therefore if an institution outsources the processing of personal information, the institution is still responsible for ensuring compliance with the POPI Act (2013). Therefore, institutions should ensure that their third party supplier contracts include clauses for recourse by the institution against the third party supplier, in the event an individual takes action against the institution for the unlawful collection, retention, dissemination and use of personal information (Monty, 2015).

The POPI Act (2013), however does not apply to the processing of personal information as it relates to purely personal or household activities, sufficiently de-identified information, specific State functions which involve State security, criminal prosecutions as well as cabinet and its committees or the executive council of a province, judicial functions and journalism, guided by a code of ethics.

3.7 REQUIREMENTS OF THE POPI ACT

In order to lawfully process personal information in South Africa, compliance with the minimum requirements of the POPI Act (2013) is required. Appendix B provides the minimum requirements for the lawful processing of personal information in South Africa as specified by the POPI Act (2013) in 12 Chapters (including 8 Conditions) consisting of 115 Sections.

The minimum requirements outlined in the POPI Act (2013) ensure the lawful collection, retention, dissemination and use of personal information. As a result, according to Monty (2015), South African institutions should ensure that personal information is collected for a specific purpose and should be relevant and updated. In addition, security measures should be implemented to ensure the confidentiality and integrity of personal information, upon request the subject to which the personal information belongs should be allowed the required access. Monty (2015) also advocates that prior consent be obtained from consumers before processing personal information and that an Information Officer be appointed to achieve and maintain compliance with the POPI Act (2013).

Of particular importance to this thesis, given the research problem identified in Chapter 1, is Condition 7 of the POPI Act (2013). The next section provides an understanding of the requirements of Condition 7 of the POPI Act (2013).

3.8 Requirements of Condition 7 of the POPI Act

Condition 7 of the POPI Act (2013) relates to security safeguards and requires institutions to ensure the confidentiality and integrity of personal information in its possession and in its control (Sikhungo, 2016). The requirements for Condition 7 of the POPI Act (2013) are outlined in 4 sections. Section 19 of the POPI Act (2013) specifies the need to implement security safeguards to ensure the confidentiality and integrity of personal information. Section 20 of the POPI Act (2013) defines the responsibilities for handling personal information. The responsibilities of an operator processing personal information are defined in Section 21 of the POPI Act (2013). Lastly, Section 22 of the POPI Act (2013) specifies the need for notification in the event of a security compromise of personal information.

3.9 Information Regulator

An Information Regulator has to be established in terms of Section 39 of the POPI Act (2013) to enforce the minimum requirements for the lawful processing of personal information in South Africa as specified by the POPI Act (2013) in 12 Chapters (including 8 Conditions). This supports Greenleaf’s (2013) recommendation that an independent “data protection authority" be established, which in the South African context is the Information Regulator, to enforce the privacy legislation as well as perform investigations relating to privacy complaints and to drive improvement of the adopted privacy legislation.

As such, the main role of the Information Regulator as per the POPI Act (2013) is to promote, enforce and monitor compliance with the POPI Act (2013). Furthermore, the POPI Act (2013) requires the Information Regulator to facilitate cross-border cooperation in the enforcement of privacy laws, conduct research and report to Parliament as well as to provide education, issue and deal with codes of conduct, consult with interested parties and handle complaints relating to the POPI Act (2013).

In 2015, processes commenced to set up the Office of the Information Regulator (Parliament of the Republic of South Africa, 2015). On 26 October 2016, the President of South Africa announced the appointment of Advocate Pansy Tlakula as the chair, Advocate Cordelia Stroom and Mr Johannes Weapond as full-time members, and Professor Tana Pistorius and Mr Sizwe Snail as part-time members of the Office of the Information Regulator, with effect from 1 December 2016 (Michalsons, 2016).

3.10 COMMENCEMENT DATE OF THE POPI ACT

At the time of completing this thesis, the commencement date of the POPI Act (2013) was still to be announced. However, the commencement date of the POPI Act (2013), as per Section 115, will be determined by the President of South Africa and there may be different dates of commencement for different provisions of the Act or with respect to the different classes of information and bodies. Since, the Office of the Information Regulator is now in place (Michalsons, 2016) the commencement date of the POPI Act (2013) may be looming on the horizon.

The "Transitional Arrangements" section of the POPI Act (2013) within Chapter 11 specifies that within 1 year of the commencement date, compliance with the Act should be achieved by public and private institutions in South Africa, unless exemptions which are gazetted are granted; however the time to comply as a result of an exemption may not exceed 3 years.

3.11 Risks Associated with the POPI Act

The POPI Act (2013) presents the risk of non-compliance. Therefore, in the event compliance with the POPI Act (2013) is not achieved, members of the South African public and private institutions may be fined up to R10 million, face imprisonment not exceeding 10 years or receive a combination of a fine and imprisonment. Furthermore, institutions may risk suffering reputational damage, loss of customers and may have to pay out millions in damages due to civil class action (Michalsons, 2014). As a result, Milo and Ampofo-Anti (2014) state that once the POPI Act (2013) is enforced: "tightening-up security measures only after a breach has occurred will become an expensive luxury, and one that may be academic if your reputation - or your wallet - doesn't survive the breach".

3.12 Opportunities Associated with the POPI Act

Chivers and Kafouris (2013) state that complying with the POPI Act (2013) is not: "just about obeying the law; it's essential to doing business in a data-driven world - and has tangible benefits for profitability and competitiveness - giving a company that gets compliant early a competitive advantage". Similarly, Rees (2016) argues from a business perspective that institutions need to manage their data better, not as a result of legislation, since doing so makes good business sense. In addition, to the aforementioned opportunities associated with the POPI Act (2013), Gerber and Skolmen (2015) highlighted that compliance with the Act may lead to an improvement in data quality from an integrity perspective, enhancement of business processes that may lead to greater efficiency, savings due to the prevention of data breaches of personal information, potential new business opportunities from institutions in the European Union (EU) as well as enhanced customer relationships and trust.

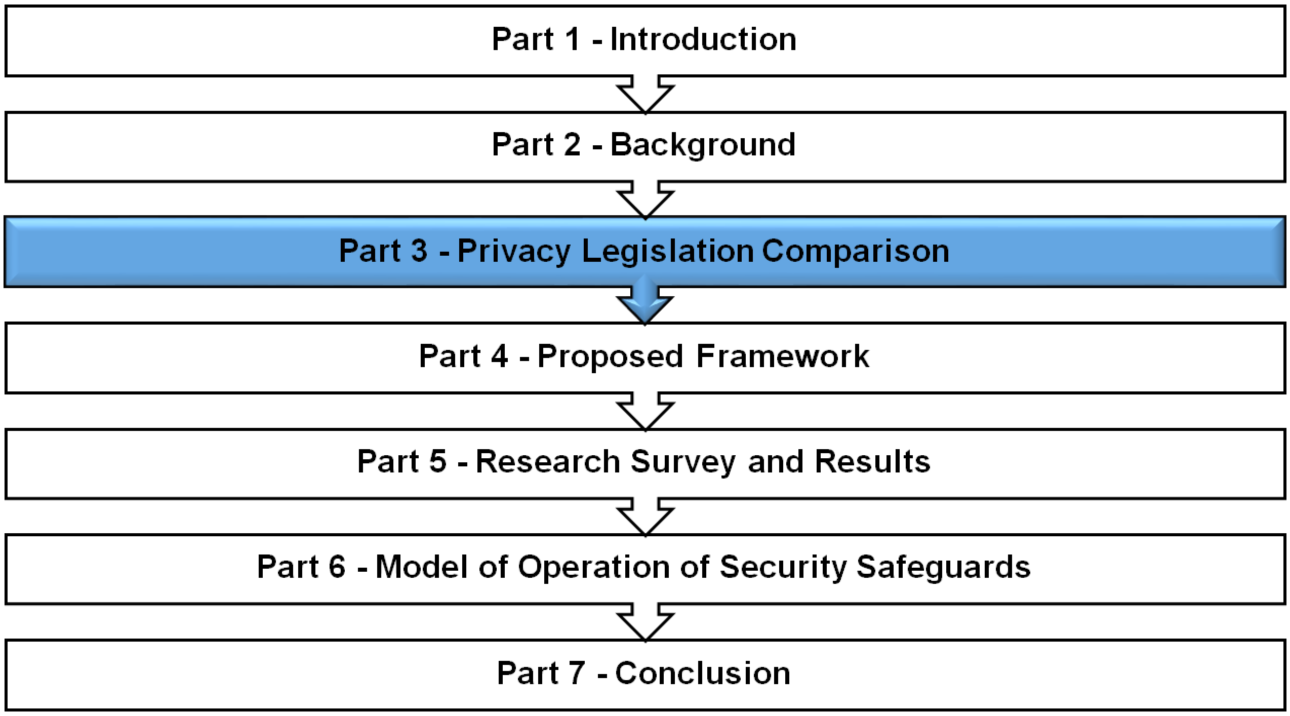
From a consumer perspective, the POPI Act (2013) provides an opportunity to protect personal information by enforcing a greater deal of accountability and responsibility on South African institutions who collect, retain, disseminate and use personal information of consumers. Most importantly for consumers, South African institutions will no longer be able to conceal a data breach, negligence or accident associated with personal information from the impacted consumers and the public at large.

3.13 Conclusion

This chapter concluded Part 2 (Background) of this thesis, by providing an overview of the South African response to privacy legislation in the form of the POPI Act (2013). In so doing, an understanding was provided in terms of the need for privacy legislation in South Africa, the country's journey from the POPI Bill to an Act, the purpose of the POPI Act (2013), personal information defined in terms of the POPI Act (2013), applicability, accountability and exclusions of the POPI Act (2013), the requirements of the POPI Act (2013) and specifically Condition 7, the establishment of an Information Regulator and the commencement date of the POPI Act (2013) followed by the risks and opportunities associated with the Act.

Part 3 (Privacy Legislation Comparison) of this thesis which consists of Chapter 4 follows this chapter and provides an analysis in terms of the extent to which the privacy legislation of the EU and South Africa addresses the international 2013 OECD guidelines.

PART 3 - PRIVACY LEGISLATION COMPARISON



Part 1 - Introduction

Part 2 - Background

Part 3 - Privacy Legislation Comparison

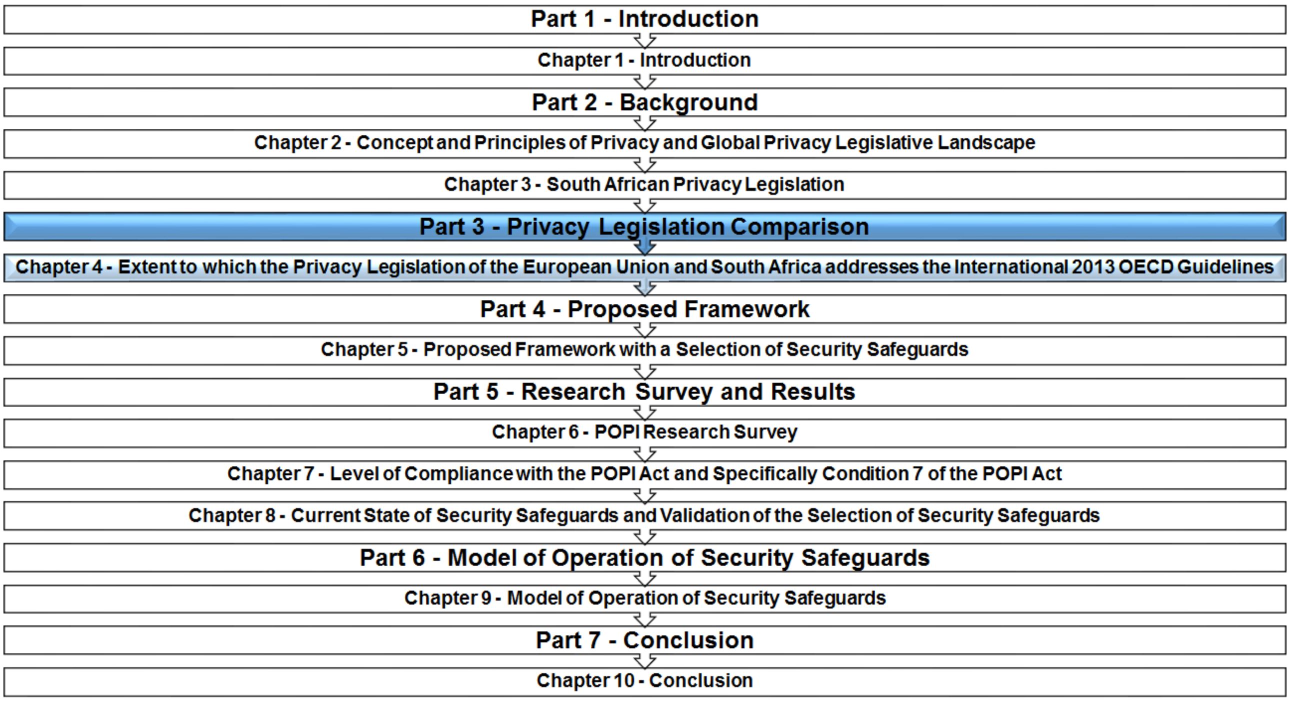
Part 4 - Proposed Framework

Part 5 - Research Survey and Results

Part 6 - Model of Operation of Security Safeguards

Part 7 - Conclusion

CHAPTER 4 - EXTENT TO WHICH THE PRIVACY LEGISLATION OF THE EUROPEAN UNION AND SOUTH AFRICA ADDRESSES THE INTERNATIONAL 2013 OECD GUIDELINES



Part 1 - Introduction

Chapter 1 - Introduction

Part 2 - Background

Chapter 2 - Concept and Principles of Privacy and Global Privacy Legislative Landscape

Chapter 3 - South African Privacy Legislation

Part 3 - Privacy Legislation Comparison

Chapter 4 - Extent to which the Privacy Legislation of the European Union and South Africa addresses the International 2013 OECD Guidelines

Part 4 - Proposed Framework

Chapter 5 - Proposed Framework with a Selection of Security Safeguards

Part 5 - Research Survey and Results

Chapter 6 - POPI Research Survey

Chapter 7 - Level of Compliance with the POPI Act and Specifically Condition 7 of the POPI Act

Chapter 8 - Current State of Security Safeguards and Validation of the Selection of Security Safeguards

Part 6 - Model of Operation of Security Safeguards

Chapter 9 - Model of Operation of Security Safeguards

Part 7 - Conclusion

Chapter 10 - Conclusion

4.1 INTRODUCTION

Chapter 2 explored the concept and principles of privacy as well as the importance of privacy and provided an overview of the global privacy legislative landscape. Chapter 3 focused on the privacy legislation adopted by South Africa in the form of the Protection of Personal Information (POPI) Act (Act 4 of 2013). This chapter addresses research question 1 - *To what extent does the privacy legislation of the European Union (EU) and South Africa address the international 2013 Organisation for Economic Co-operation and Development (OECD) guidelines?*

In so doing, the rationale for analysing the extent to which the privacy legislation of the EU and South Africa addresses the international 2013 OECD guidelines on trans-border data flows and the protection of privacy, is provided. This is followed by an overview of the OECD international guidelines on trans-border data flows and the protection of privacy as well as the EU and South African privacy legislation. Thereafter, an analysis is performed to address the extent to which the privacy legislation of the EU and South Africa address the international 2013 OECD guidelines on trans-border data flows and the protection of privacy. Lastly, this analysis gives rise to a critical evaluation in terms of the similarities and differences associated with the privacy legislation compared in this chapter.

4.2 RATIONALE

Several researchers such as Dowling (2009), De Bruyn (2014), and Botha et al. (2015) have compared the privacy legislation of specific countries or regions. Dowling (2009) compared the EU privacy legislation, the Data Protection Directive (1995), to several countries within Europe and around the globe. De Bruyn (2014) compared the POPI Act (2013) (limited to the 8 conditions) to the privacy legislation of the United Kingdom. Botha et al. (2015) compared the POPI Act (2013) (limited to the 8 conditions) to the privacy legislation of the EU as well as the United Kingdom, United States of America (USA) and Australia.

However, at the time of conducting research as part of this thesis, the extent to which the EU and South African privacy legislation addresses the international 2013 OECD guidelines on trans-border data flows and the protection of privacy, which includes the 8 privacy principles, had not been explored. Furthermore, the rationale for selecting the EU privacy legislation for comparison as part of this research is due to South African privacy legislation favouring the European concept to protect personal information as cited by Stein (2012) and Perumall (2013), and which according to Birnhack (2008) was largely motivated by international trade and for participation in the global economy (Roos, 2007).

4.3 OVERVIEW

This section provides an overview of the OECD international guidelines on trans-border data flows and the protection of privacy as well as the EU and South African privacy legislation as these form the basis for the comparison as part of the analysis conducted in this chapter.

4.3.1 THE INTERNATIONAL OECD GUIDELINES ON TRANS-BORDER DATA FLOWS AND THE PROTECTION OF PRIVACY

As mentioned in Chapter 2, in 1980 the OECD adopted international guidelines on trans-border data flows and the protection of privacy. The guidelines included 8 privacy principles (collection, data quality, purpose specification, use limitation, security safeguards, openness, individual participation and accountability) to govern the preservation of privacy and trans-border flow of personal data (OECD, 1980). The international guidelines on trans-border data flows and the protection of privacy were revised by the OECD in 2013 to make provision for the basic principles of international application in terms of free flow and legitimate restrictions, national implementation, international co-operation and interoperability as well as implementing accountability (OECD, 2013). The 8 privacy principles prescribed within the international guidelines by the OECD in 1980 remained unchanged in the 2013 revision (Kuschewsky, 2014).

4.3.2 European Union Privacy Legislation

Privacy legislation in the EU takes the form of the Data Protection Directive (also known as Directive 95/46/EC) of 1995. The purpose of the Data Protection Directive (1995) as outlined in Article 1 is to ensure that: "member states shall protect the fundamental rights and freedoms of natural persons, and in particular, their right to privacy with respect to the processing of personal data." In addition, the Data Protection Directive (1995) encourages the free flow of personal data between member states as long as privacy is preserved.

Article 2 of the Data Protection Directive (1995) defines personal data as: "any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."

The protection of personal data as promoted by the Data Protection Directive (1995) is applicable to all EU member states. However, each EU member state enacts their own privacy laws based on the Data Protection Directive (1995), utilising the 7 Chapters (including 34 Articles) as provided in Appendix C of this thesis.

The Data Protection Directive (1995) is not a regulation and this has allowed EU member states to interpret and apply the Directive in an inconsistent manner within their own enacted privacy legislation (Lynch, 2013). For example, Chapter 3 of the Directive (1995) makes provision for judicial remedies, liability and sanctions, however the conditions, actual penalties and enforcement in the event of a breach of personal information differs for each EU member state.

As a result, in 2012 the European Commission proposed that the Data Protection Directive (1995) be replaced by the General Data Protection Regulation (2012). This proposal marked a paradigm shift from "directive" to "regulation" that sought to provide a single data protection law applicable to all EU member states, thus preventing the need for individual privacy legislation by each member state. Greens (2015) envisaged that the General Data

Protection Regulation will be adopted by the end of 2015 and will be followed by a two-year transition period to allow EU member states to comply, followed by the enforcement of the regulation. During the course of this thesis, on 27 April 2016 the European Parliament published the General Data Protection Regulation (2016) which will be effective from 25 May 2018 within all EU member states.

4.3.3 South African Privacy Legislation

The South African privacy legislation was finally enacted and signed into law on 26 November 2013 as the POPI Act (2013). Chapter 3 of this thesis provides a detailed overview of the POPI Act (2013). In summary, the POPI Act (2013) promotes the lawful processing of personal information by South African public and private institutions as per the minimum requirements specified within 12 Chapters (including 8 Conditions), as reflected in Appendix B. An Information Regulator has to be established in terms of Section 39 of the POPI Act (2013) to promote, enforce and monitor compliance with the Act. Although the POPI Act (2013) was signed into law on 26 November 2013, the commencement date of the Act is still to be announced.

4.4 Analysis of the European Union and South African Privacy Legislation in Relation to the International 2013 OECD Guidelines

The analysis uses the OECD's 8 privacy principles (collection, data quality, purpose specification, use limitation, security safeguards, openness, individual participation and accountability) as well as the additional focus areas (implementing accountability, basic principles of international application in terms of free flow and legitimate restrictions, national implementation and international co-operation and interoperability) of the international 2013 OECD guidelines on trans-border data flows and the protection of privacy, as the basis for comparison.

As a result, Table 4.1 on the next page provides the first component of the analysis, which evaluates the extent to which the EU Data Protection Directive (1995) addresses the international 2013 OECD guidelines.

Table 4.1: Extent to which the EU Data Protection Directive addresses the International 2013 OECD Guidelines

Number	**Description of the international 2013 OECD guideline on trans-border data flows and the protection of privacy**	**Requirement addressed by the EU Data Protection Directive of 1995**
1	Privacy principle: Collection limitation	**Yes** - Chapter 2: General rules on the lawfulness of the processing of personal data (Articles 5 and 6).
2	Privacy principle: Data quality	**Yes** - Chapter 2: General rules on the lawfulness of the processing of personal data (Article 6).
3	Privacy principle: Purpose specification	**Yes** - Chapter 2: General rules on the lawfulness of the processing of personal data (Articles 6, 7, 8, 9, 10 and 11).
4	Privacy principle: Use limitation	**Yes** - Chapter 2: General rules on the lawfulness of the processing of personal data (Articles 6, 7, 8, 9, 10, 11, 20 and 21).
5	Privacy principle: Security safeguards	**Yes** - Chapter 2: General rules on the lawfulness of the processing of personal data (Articles 16 and 17).
6	Privacy principle: Openness	**Yes** - Chapter 2: General rules on the lawfulness of the processing of personal data (Articles 12 and 13).
7	Privacy principle: Individual participation	**Yes** - Chapter 2: General rules on the lawfulness of the processing of personal data (Articles 14 and 15).
8	Privacy principle: Accountability	**Yes** - Chapter 1: General provisions (Article 4) and Chapter 2: General rules on the lawfulness

Number	Description of the international 2013 OECD guideline on trans-border data flows and the protection of privacy	Requirement addressed by the EU Data Protection Directive of 1995
		of the processing of personal data (Article 6).
9	Other focus areas: Implementing accountability - Privacy management programme	**No** - Specific reference is not made to a privacy management programme.
10	Other focus areas: Implementing accountability - Privacy enforcement authorities	**Yes** - Chapter 6: Supervisory authority and working party on the protection of individuals with regard to the processing of personal data (Article 28).
11	Other focus areas: Implementing accountability - Data security breach notification	**Yes** - Chapter 2: General rules on the lawfulness of the processing of personal data (Article 18).
12	Other focus areas: Basic principles of international application in terms of free flow and legitimate restrictions - Trans-border flows of personal data	**Yes** - Chapter 4: Transfer of personal data to third countries (Articles 25 and 26).
13	Other focus areas: National implementation	**No** - The European Union Data Protection Directive is not a regulation; it is a directive. As a result, Chapter 1: Article 4 states that each member state shall apply the national provisions it adopts pursuant to the directive.
14	Other focus areas:	**Yes** - Chapter 4: Transfer of personal data to

Number	Description of the international 2013 OECD guideline on trans-border data flows and the protection of privacy	Requirement addressed by the EU Data Protection Directive of 1995
	International co-operation and interoperability	third countries (Articles 25 and 26).

As per Table 4.1 above, the EU Data Protection Directive (1995) addresses the 8 privacy principles from the international 2013 OECD guidelines on trans-border data flows and the protection of privacy. However, the EU Data Protection Directive (1995) does not make reference to a privacy management programme to address the national implementation requirement as it is not a regulation; it is a directive.

Similarly, Table 4.2 below provides the second component of the analysis, which evaluates the extent to which the South African POPI Act (2013) addresses the international 2013 OECD guidelines.

Table 4.2: Extent to which the South African POPI Act addresses the International 2013 OECD Guidelines

Number	Description of the international 2013 OECD guideline on trans-border data flows and the protection of privacy	Requirement addressed by the South African POPI Act
1	Privacy principle: Collection limitation	**Yes** - Chapter 3: Conditions for lawful processing of personal information (Conditions 2, 3 and 4).
2	Privacy principle: Data quality	**Yes** - Chapter 3: Conditions for lawful processing of personal information (Condition

Number	Description of the international 2013 OECD guideline on trans-border data flows and the protection of privacy	Requirement addressed by the South African POPI Act
		5).
3	Privacy principle: Purpose specification	**Yes** - Chapter 3: Conditions for lawful processing of personal information (Conditions 3 and 4).
4	Privacy principle: Use limitation	**Yes** - Chapter 3: Conditions for lawful processing of personal information (Conditions 2, 3 and 4) and Chapter 6: Prior authorisation.
5	Privacy principle: Security safeguards	**Yes** - Chapter 3: Conditions for lawful processing of personal information (Condition 7).
6	Privacy principle: Openness	**Yes** - Chapter 3: Conditions for lawful processing of personal information (Condition 6).
7	Privacy principle: Individual participation	**Yes** - Chapter 3: Conditions for lawful processing of personal information (Condition 8).
8	Privacy principle: Accountability	**Yes** - Chapter 3: Conditions for lawful processing of personal information (Condition 1).
9	Other focus areas: Implementing accountability - Privacy management programme	**No** - Specific reference is not made to a privacy management programme. However, chapter 11 makes reference to an administrative fine being enforced in the event of failure to conduct a risk assessment and maintain good policies, procedures and practices to protect personal

Number	Description of the international 2013 OECD guideline on trans-border data flows and the protection of privacy	Requirement addressed by the South African POPI Act
		information.
10	Other focus areas: Implementing accountability - Privacy enforcement authorities	**Yes** - Chapter 5: Information regulator.
11	Other focus areas: Implementing accountability - Data security breach notification	**Yes** - Chapter 3: Conditions for lawful processing of personal information (Condition 7).
12	Other focus areas: Basic principles of international application in terms of free flow and legitimate restrictions - Trans-border flows of personal data	**Yes** - Chapter 9: Trans-border information flows.
13	Other focus areas: National implementation	**Yes** - The Protection of Personal Information Act is applicable to all public and private institutions in South Africa. At this stage the Act was signed into law on 26 November 2013. The enforcement date for the POPI Act (2013) is still to be announced. Thereafter, a one year transition period will apply to allow all public and private institutions in South Africa to comply with the POPI Act (2013), after which enforcement will be monitored by the

Number	Description of the international 2013 OECD guideline on trans-border data flows and the protection of privacy	Requirement addressed by the South African POPI Act
		Information Regulator.
14	Other focus areas: International co-operation and interoperability	**Yes** - Chapter 5: Information regulator (co-operating on a national and international basis with other persons and bodies concerned with the protection of personal information).

In terms of the South African POPI Act (2013) as per Table 4.2 above, the international 2013 OECD guidelines on trans-border data flows and the protection of privacy, including the 8 privacy principles are addressed. The only exception is that no specific reference is made to a privacy management programme within the POPI Act (2013). However, reference is made to an administrative fine being enforced in the event of failure to conduct a risk assessment and maintain good policies, procedures and practices to protect personal information.

4.5 CRITICAL EVALUATION - SIMILARITIES AND DIFFERENCES

The critical evaluation of the extent to which the privacy legislation of the EU and South Africa addresses the international 2013 OECD guidelines, led to the identification of similarities and differences between these pieces of legislation.

The EU's privacy legislation which takes the form of the Data Protection Directive (1995) and the South African privacy legislation in the form of the POPI Act (2013) are similar in that both address all 8 privacy principles (collection, data quality, purpose specification, use limitation, security safeguards, openness, individual participation and accountability) specified within the international 2013 OECD guidelines on trans-border data flows and the protection of privacy. The provision of the 8 privacy principles by the Data Protection

Directive (1995) and the POPI Act (2013) is critical, as according to Greenleaf (2013), data privacy laws can only be effective if they include a comprehensive set of data privacy principles that are compliant with international standards, such as the 8 privacy principles specified within the international 2013 OECD guidelines on trans-border data flows and the protection of privacy.

Furthermore, the Data Protection Directive (1995) and the POPI Act (2013) are similar in that both do not make provision for a privacy management programme as specified within the international 2013 OECD guidelines on trans-border data flows and the protection of privacy. An adequate privacy management programme has to be defined, implemented and subjected to review from a privacy enforcement authority to uphold the accountability privacy principle and ensure that notice is provided to the privacy enforcement authority in the event of a breach of personal data (OECD, 2013). However, from a POPI Act (2013) perspective, to overcome the shortcoming related to the lack of a privacy management programme, Chapter 11 of the POPI Act (2013), makes reference to an administrative fine being enforced in the event of failure to conduct a risk assessment and to maintain good policies, procedures and practices to protect personal information. In addition, a privacy enforcement authority in the form of the Information Regulator, as specified in Chapter 5 of the POPI Act (2013), is required to monitor enforcement and receive notifications relating to breaches of personal data.

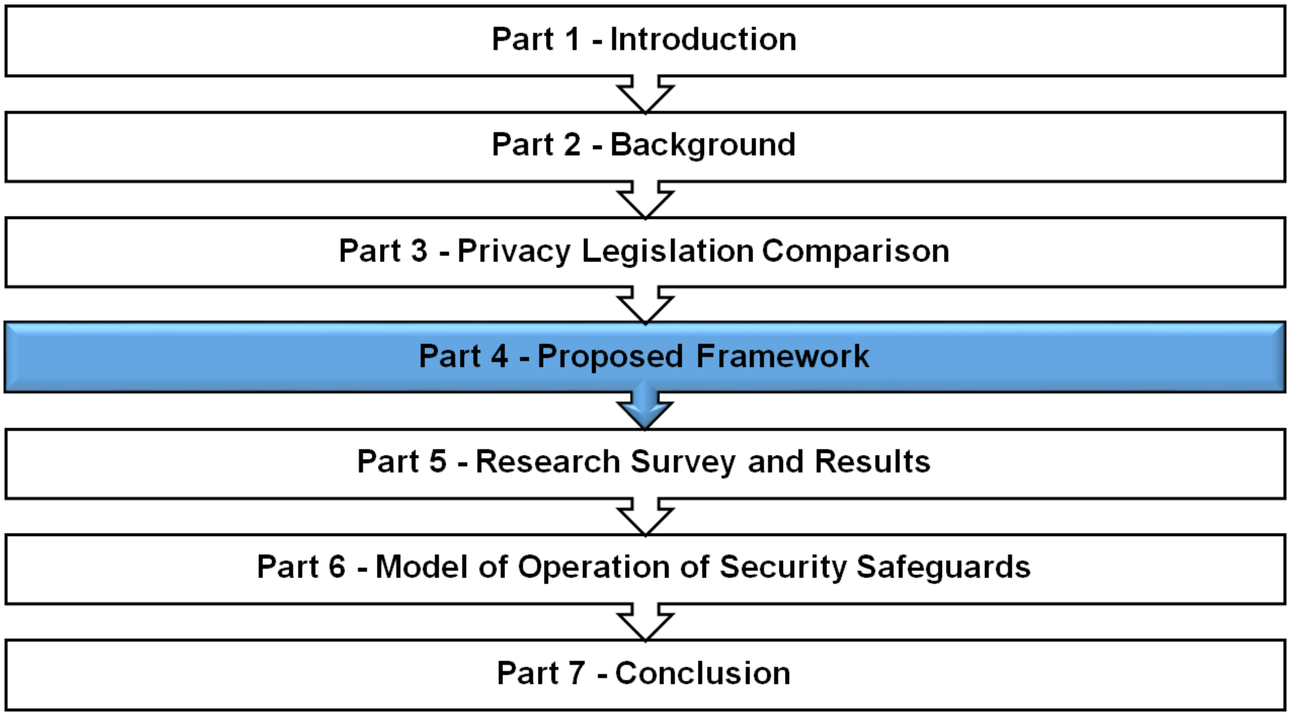
The major difference between the Data Protection Directive (1995) and the POPI Act (2013) is that the latter is enforceable, compared to the Data Protection Directive (1995) which is not enforceable. As such, the national implementation requirement as specified within the international 2013 OECD guidelines on trans-border data flows and the protection of privacy is addressed by the POPI Act (2013), compared to the Data Protection Directive (1995) where it is not addressed. This is due to the Data Protection Directive (1995) not being enforceable as it is a directive rather than a regulation and, as such, is viewed as a guideline to serve as a frame of reference for EU member states when developing and enacting their own privacy legislation. However, this shortcoming is being addressed by the General Data Protection Regulation (2016) which was published on 27 April 2016 and will become effective from 25 May 2018 within all EU member states.

4.6 CONCLUSION

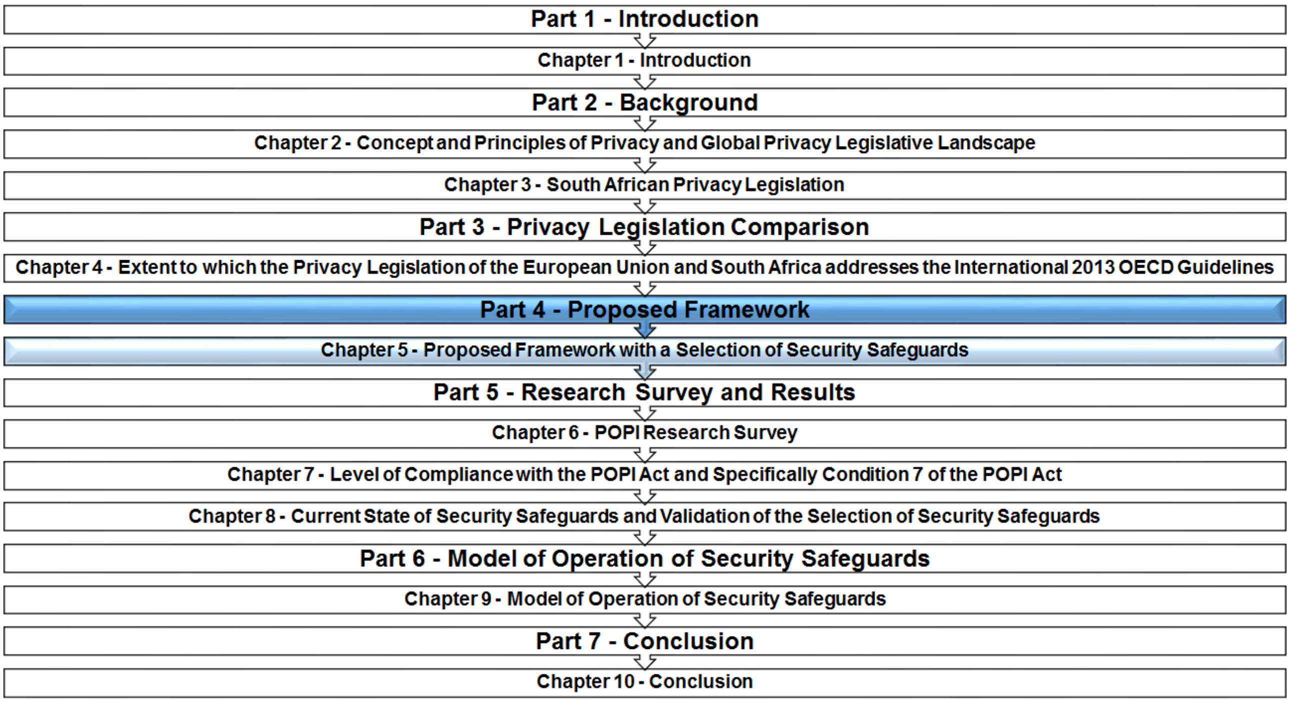
Part 3 (Privacy Legislation Comparison) of this thesis was concluded in terms of Chapter 4, which provided the rationale for analysing the extent to which the EU and South African privacy legislation addresses the international 2013 OECD guidelines on trans-border data flows and the protection of privacy. This was followed by an overview of the OECD international guidelines on trans-border data flows and the protection of privacy as well as the EU and South African privacy legislation. Thereafter, the research question associated with this chapter was addressed by analysing the extent to which EU and South African privacy legislation respectively address the international 2013 OECD guidelines on trans-border data flows and the protection of privacy. Lastly, a critical evaluation in terms of the similarities and differences associated with the privacy legislation compared within the chapter was provided.

This chapter is followed by Part 4 (Proposed Framework) of this thesis, which consists of Chapter 5 that proposes a framework that includes a selection of security safeguards to ensure confidentiality and integrity of electronic personal information in order to achieve and maintain compliance with Condition 7 of the POPI Act (2013).

PART 4 - PROPOSED FRAMEWORK


Part 1 - Introduction
Part 2 - Background
Part 3 - Privacy Legislation Comparison
Part 4 - Proposed Framework
Part 5 - Research Survey and Results
Part 6 - Model of Operation of Security Safeguards
Part 7 - Conclusion

CHAPTER 5 - PROPOSED FRAMEWORK WITH A SELECTION OF SECURITY SAFEGUARDS



Part 1 - Introduction

Chapter 1 - Introduction

Part 2 - Background

Chapter 2 - Concept and Principles of Privacy and Global Privacy Legislative Landscape

Chapter 3 - South African Privacy Legislation

Part 3 - Privacy Legislation Comparison

Chapter 4 - Extent to which the Privacy Legislation of the European Union and South Africa addresses the International 2013 OECD Guidelines

Part 4 - Proposed Framework

Chapter 5 - Proposed Framework with a Selection of Security Safeguards

Part 5 - Research Survey and Results

Chapter 6 - POPI Research Survey

Chapter 7 - Level of Compliance with the POPI Act and Specifically Condition 7 of the POPI Act

Chapter 8 - Current State of Security Safeguards and Validation of the Selection of Security Safeguards

Part 6 - Model of Operation of Security Safeguards

Chapter 9 - Model of Operation of Security Safeguards

Part 7 - Conclusion

Chapter 10 - Conclusion

5.1 INTRODUCTION

Chapter 4 assessed the extent to which the privacy legislation of the European Union (EU) and South Africa addresses the international 2013 Organisation for Economic Co-operation and Development (OECD) guidelines on trans-border data flows and the protection of privacy. This chapter addresses research question 2 - *How can South African institutions, who store, process and transmit electronic personal information achieve and maintain compliance with Condition 7 of the POPI Act (2013), including the security safeguards to be considered to ensure confidentiality and integrity of electronic personal information?*

This chapter proposes a framework that encapsulates a selection of security safeguards to ensure confidentiality and integrity of electronic personal information stored, processed or transmitted. In doing so, the requirements of Condition 7 of the POPI Act (2013) are provided followed by an overview and basis for the proposed framework as well as a description of each phase of the proposed framework, including a selection of security safeguards. In addition, a critical evaluation in terms of the benefits and limitations associated with the proposed framework is provided.

5.2 REQUIREMENTS OF CONDITION 7 OF THE POPI ACT

Condition 7 of the POPI Act (2013) specifically requires the implementation of security safeguards to ensure the confidentiality and integrity of personal information (Section 19), the definition of responsibilities for handling personal information (Section 20), clear responsibilities for an operator processing personal information (Section 21) as well as the need for notification in the event of a security compromise of personal information (Section 22).

However, as per the research problem identified in Chapter 1, the legislative requirement of Condition 7 of the POPI Act (2013) defined in sections 19, 20, 21 and 22 is not supported by specific guidance in terms of how the requirement should be satisfied. There is also no specific guidance on the security safeguards, as required in Section 19, to ensure the confidentiality and integrity of specifically electronic personal information for the purpose of this thesis.

5.3 Overview of the Proposed POPI Condition 7 Framework

In order to address the research question in this Chapter as a result of the shortcoming of Condition 7 of the POPI Act (2013), in terms of specific guidance to achieve the requirements of sections 19, 20, 21 and 22, the "POPI Condition 7 framework" as illustrated in Figure 5.1 below is proposed. This framework provides in 4 distinct phases ("Identify", "Secure", "Monitor and Report" and "Remediate") an approach, which includes a specific selection of security safeguards as part of the "Secure" phase, to ultimately address the requirements of Condition 7 of the POPI Act (2013), specifically in relation to electronic personal information.

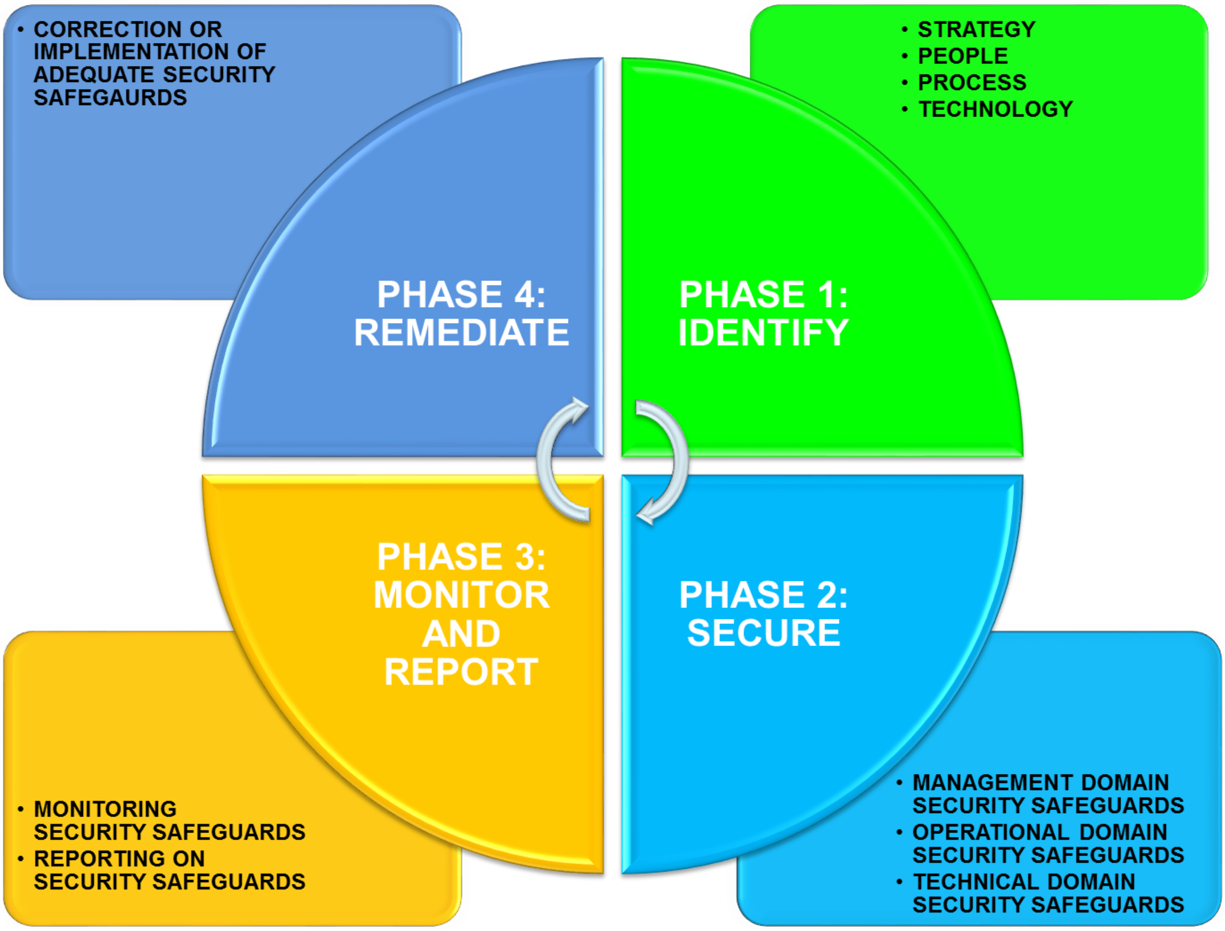

• CORRECTION OR IMPLEMENTATION OF ADEQUATE SECURITY SAFEGAURDS
• STRATEGY
• PEOPLE
• PROCESS
• TECHNOLOGY
PHASE 4: REMEDIATE
PHASE 1: IDENTIFY
PHASE 3: MONITOR AND REPORT
PHASE 2: SECURE
• MONITORING SECURITY SAFEGUARDS
• REPORTING ON SECURITY SAFEGUARDS
• MANAGEMENT DOMAIN SECURITY SAFEGUARDS
• OPERATIONAL DOMAIN SECURITY SAFEGUARDS
• TECHNICAL DOMAIN SECURITY SAFEGUARDS

Figure 5.1: Proposed POPI Condition 7 Framework to Address the Requirements of Condition 7 of the POPI Act in Relation to Electronic Personal Information

The "Identify" phase of the proposed POPI Condition 7 framework is focused on the identification of electronic personal information. This is followed by the "Secure" phase that aims to secure electronic personal information, which has been identified that needs to be protected through the selection and implementation of security safeguards. The next phase, "Monitor and Report", ensures that electronic personal information remains protected and in instances when the protection is not in place, this should be reported in order to initiate remedial action. The final phase, "Remediate", addresses remedial action to ensure that the protection of electronic personal information is maintained.

5.4 Basis of the Proposed POPI Condition 7 Framework

The 4-phased approach taken in the POPI Condition 7 framework leverages off the principles from the quality assurance model known as Plan-Do-Check-Act (PDCA) applied to the International Organisation for Standardisation (ISO) management system standards (British Standards Institute (BSI), 2013) as illustrated in Figure 5.2 below.

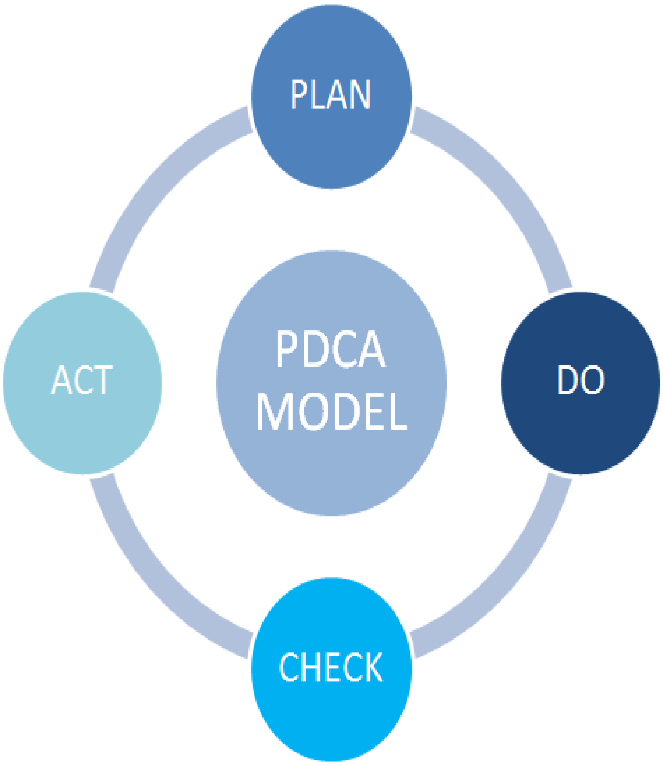


Figure 5.2: Plan-Do-Check-Act (PDCA) Model

Source: Adapted from BSI (2014)

The "Plan" phase analyses the current environment, establishes objectives, sets interim targets for review and defines plans to achieve these targets (BSI, 2013). This is followed by the "Do" phase which is focused on the implementation of the defined plans. The "Check" phase measures the actual results against planned objectives (BSI, 2013). Lastly, the "Act" phase aims to correct and improve plans to meet or exceed planned objectives (BSI, 2013).

The PDCA model was adopted in an information security context in terms of the ISO 27001 standard (BSI, 2005). The ISO 27001 standard (BSI, 2005) prescribed the use of the PDCA model to implement an information security management system (ISMS) as a means to effectively manage the information assets of an organisation. Electronic personal information is an information asset and the 4-phased approach of the proposed POPI Condition 7 framework for protecting electronic personal information is closely aligned to the principles of the PDCA model. Table 5.1 below, provides a description of each phase of the PDCA model in terms of implementing an ISMS and the alignment to the 4 phases of the proposed POPI Condition 7 framework.

Table 5.1: Alignment between the Phases of the PDCA Model and the Proposed POPI Condition 7 Framework

Number	PDCA phase	Proposed POPI Condition 7 framework phase
1	Plan - Establish an ISMS.	"Identify" - Identification of electronic personal information.
2	Do - Implement and operate the ISMS.	"Secure" - Securing the electronic personal information identified that needs to be protected through the selection and implementation of security safeguards.
3	Check - Monitor and review the ISMS.	"Monitor and Report" - Monitoring and reporting to ensure that the electronic personal information remains protected and instances when the protection is not in place this should be reported in order to initiate remedial action.

Number	PDCA phase	Proposed POPI Condition 7 framework phase
4	Act - Maintain and improve the ISMS.	"Remediate" - Remedial action taken to ensure the protection of electronic personal information is maintained.

5.5 Phases of the Proposed POPI Condition 7 Framework with a Selection of Security Safeguards

The 4 distinct phases ("Identify", "Secure", "Monitor and Report" and "Remediate") of the proposed POPI Condition 7 framework with a specific selection of security safeguards as part of the "Secure" phase, address the requirements of Condition 7 of the POPI Act (2013), specifically in relation to electronic personal information. Subsections 5.5.1 to 5.5.4 unpacks each phase of the proposed POPI Condition 7 framework. Furthermore, the specific selection of security safeguards is provided as part of the "Secure" phase of the proposed POPI Condition 7 framework within subsection 5.5.2.3.

5.5.1 Phase 1: Identify

Phase 1 ("Identify") of the proposed POPI Condition 7 framework focuses on the identification of electronic personal information and consists of 4 key perspectives: Strategy, People, Process and Technology as illustrated in Figure 5.3 below.

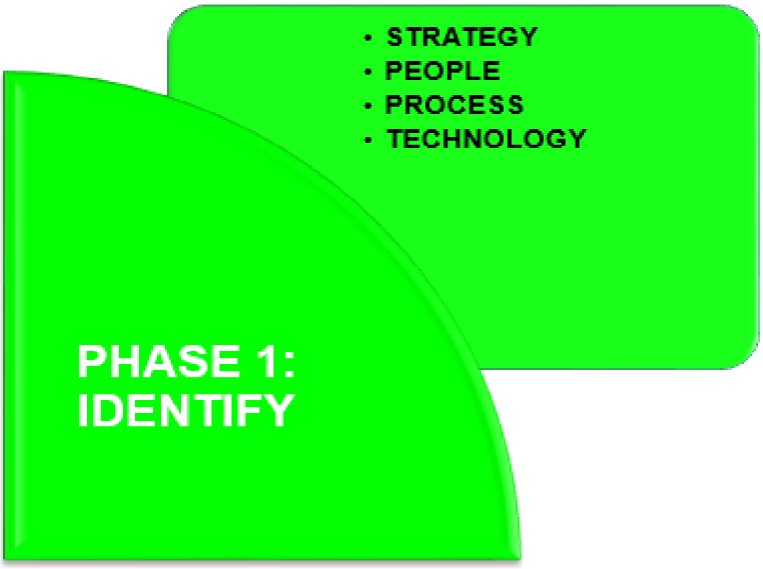


Figure 5.3: Proposed POPI Condition 7 Framework - Phase 1 (Identify)

The key perspectives as illustrated in Figure 5.3 are unpacked below from subsection 5.5.1.1 to 5.5.1.4.

5.5.1.1 Strategy Perspective

The strategic perspective considers whether an institution has identified the threats and vulnerabilities associated with the storage, processing and transmission of electronic personal information and developed a strategy to mitigate the risk, thereby demonstrating strategic intent to comply and maintain compliance with Condition 7 of the POPI Act (2013).

5.5.1.2 People Perspective

From a people perspective, this phase questions whether the relevant internal and external stakeholders have been identified who will drive the initiative to comply and maintain compliance with Condition 7 of the POPI Act (2013).

5.5.1.3 Process Perspective

The process perspective consists of the identification of manual and automated business processes within the institution which store, process and transmit personal information as defined by the POPI Act (2013). Thereafter, the personal information identified should be categorised as personal information that is stored, processed and transmitted in electronic format (within information systems and their corresponding databases) as opposed to non-electronic format (hard copy or paper based outside information systems).

5.5.1.4 Technology Perspective

Lastly, the technology perspective identifies the extent to which technology may be leveraged to safeguard electronic personal information.

The “Identify” phase of the proposed POPI Condition 7 framework is followed by the “Secure” phase as discussed below.

5.5.2 Phase 2: Secure

Phase 2 (“Secure”) is premised on selecting security safeguards commonly referred to as security controls to ensure the confidentiality and integrity of electronic personal information identified in Phase 1 (“Identify”). This subsection, provides a definition for a security safeguard and the source of the selection of security safeguards. This is followed by the specific selection of security safeguards within 3 domains (management, operational and technical) to ultimately address the requirements of Condition 7 of the POPI Act (2013), specifically in relation to electronic personal information. Lastly, a summary and the source of the specific selection of security safeguards within the 3 domains (management, operational and technical), which form part of the “Secure” phase of the proposed POPI Condition 7 framework is provided.

5.5.2.1 Definition of a Security Safeguard

A security safeguard, commonly referred to as a control as per the Control Objectives for Information and related Technology (COBIT) framework (ISACA, 2007), is defined as: “policies, procedures, practices and organisational structures designed to provide reasonable assurance that business objectives will be achieved and that undesired events will be prevented or detected and corrected.” In line with the definition provided by the COBIT framework (ISACA, 2007), preventative, detective and corrective control categories exist. Preventative controls are designed to prevent the unauthorised disclosure and manipulation of electronic personal information (ISACA, 2014b). In comparison, a detective control intends to detect while corrective controls aim to correct a scenario of unauthorised disclosure and manipulation of electronic personal information (ISACA, 2014b). Furthermore, preventative, detective and corrective controls may be classified as technical (for example a firewall) or non-technical (for example, an information security policy or data classification policy) (ISACA, 2014b).

5.5.2.2 Source of the Selection of Security Safeguards

The source of the selection of security safeguards within the “Secure” phase is derived from several leading practices formulated by leading practice institutions including the Information Systems Audit and Control Association (ISACA), the National Institute of

Standards and Technology (NIST), the Office of Government Commerce United Kingdom (OGCUK) and the International Organisation for Standardisation (ISO). These leading practices which serve as a source for the selection of security safeguards are grouped by leading practice institutions and unpacked from subsections 5.5.2.2.1 to 5.5.2.2.4 to follow.

5.5.2.2.1 INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION (ISACA)

ISACA first introduced the COBIT framework in 1996 with a primary focus on audit (Stroud, 2012). From 1996, the COBIT framework evolved into COBIT 2 in 1998, which focused on controls to COBIT 3 in 2000, which expanded to include the management aspects of information technology, to COBIT 4.1 in 2007 which highlighted information technology governance. The latest version of the COBIT framework, COBIT 5, was released in 2012 and focuses on the governance of enterprise information technology (Stroud, 2012) by creating optimal value from information technology through maintaining a balance between releasing benefits, optimising risk levels and resource usage (ISACA, 2014c).

The governance and management of enterprise information technology is underpinned by 5 key principles within COBIT 5 - namely, meeting stakeholder needs, covering the enterprise end to end, applying a single integrated framework, enabling a holistic approach and separating governance from management (ISACA, 2014c). These 5 principles are complemented by a series of enablers - principles, policies and frameworks, processes, organisational structures, culture, ethics and behavior, information, services, infrastructure and applications as well as people, skills and competencies (ISACA, 2014c). In addition, as illustrated in Figure 5.4 on the next page, COBIT 5 (ISACA, 2014c) consists of 5 governance processes encapsulated within the evaluate, direct and monitor (EDM) domain as well as 32 management processes encapsulated within 4 domains - align, plan and organise (APO), build, acquire and implement (BAI), deliver, service and support (DSS) and monitor, evaluate and assess (MEA).

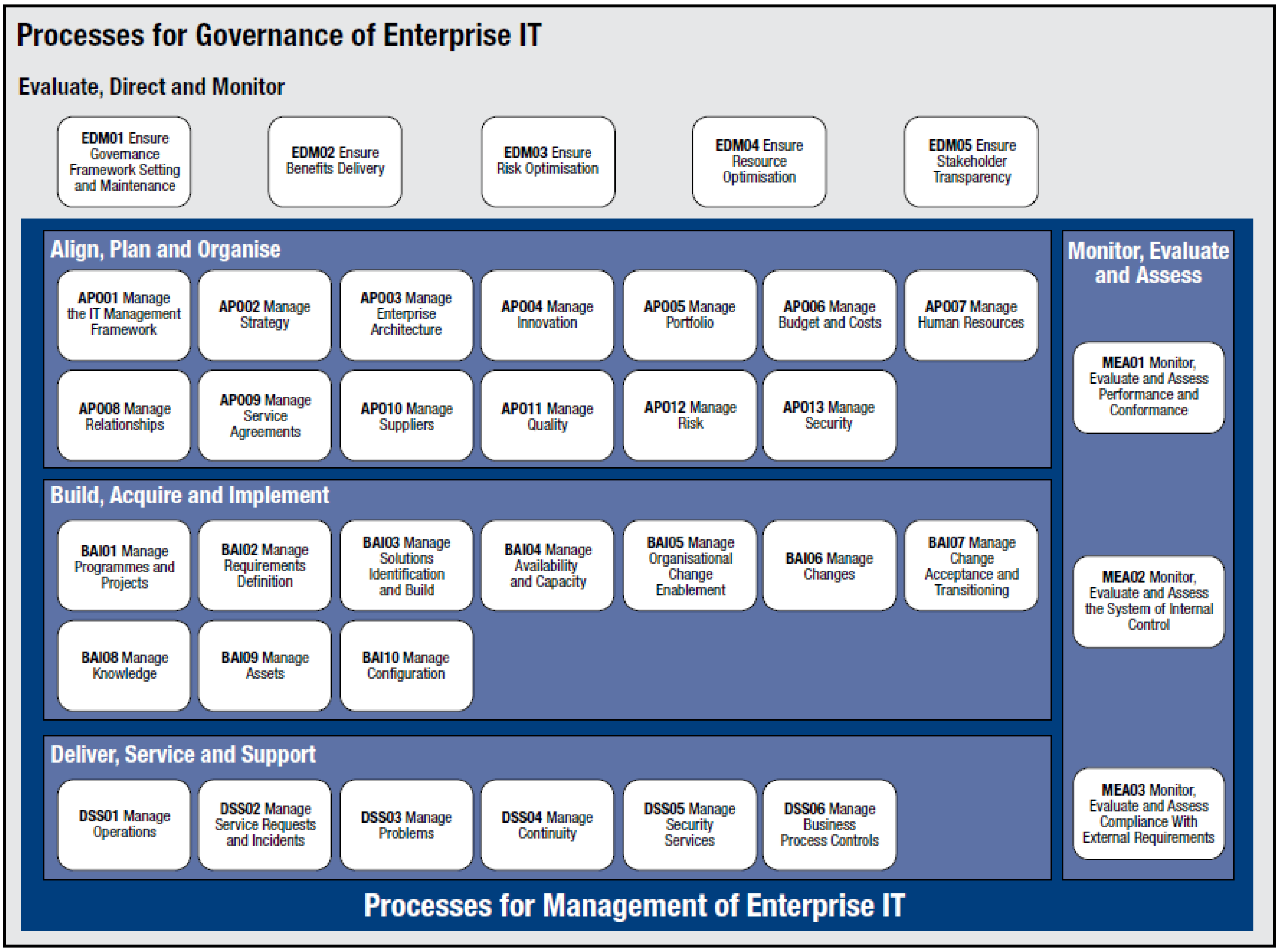

Processes for Governance of Enterprise IT
Evaluate, Direct and Monitor
EDM01 Ensure Governance Framework Setting and Maintenance
EDM02 Ensure Benefits Delivery
EDM03 Ensure Risk Optimisation
EDM04 Ensure Resource Optimisation
EDM05 Ensure Stakeholder Transparency
Align, Plan and Organise
APO01 Manage the IT Management Framework
APO02 Manage Strategy
APO03 Manage Enterprise Architecture
APO04 Manage Innovation
APO05 Manage Portfolio
APO06 Manage Budget and Costs
APO07 Manage Human Resources
APO08 Manage Relationships
APO09 Manage Service Agreements
APO10 Manage Suppliers
APO11 Manage Quality
APO12 Manage Risk
APO13 Manage Security
Monitor, Evaluate and Assess
MEA01 Monitor, Evaluate and Assess Performance and Conformance
MEA02 Monitor, Evaluate and Assess the System of Internal Control
MEA03 Monitor, Evaluate and Assess Compliance With External Requirements
Build, Acquire and Implement
BAI01 Manage Programmes and Projects
BAI02 Manage Requirements Definition
BAI03 Manage Solutions Identification and Build
BAI04 Manage Availability and Capacity
BAI05 Manage Organisational Change Enablement
BAI06 Manage Changes
BAI07 Manage Change Acceptance and Transitioning
BAI08 Manage Knowledge
BAI09 Manage Assets
BAI10 Manage Configuration
Deliver, Service and Support
DSS01 Manage Operations
DSS02 Manage Service Requests and Incidents
DSS03 Manage Problems
DSS04 Manage Continuity
DSS05 Manage Security Services
DSS06 Manage Business Process Controls
Processes for Management of Enterprise IT

Figure 5.4: COBIT 5 Process Reference Model

Source: ISACA (2014c)

Furthermore, ISACA also developed the Risk IT framework in 2009 to provide guiding principles to identify, govern and effectively manage IT risk within institutions (ISACA, 2009). The guiding principles of the Risk IT framework includes a connection to business objectives, alignment of IT risk management with overall enterprise risk management, balancing the costs and benefits of managing IT risk, promoting fair and open communication of IT risk, establishing the right tone and accountability at the top as well as embedding the IT risk management process into daily activities (ISACA, 2009). In addition, the Risk IT framework (ISACA, 2009) is supported by a process model that includes 3 domains (risk governance, risk evaluation and risk response) with each domain consisting of 3 processes (the risk governance domain - to establish and maintain a common risk view, integrate with enterprise risk management and make risk aware business decisions, the risk evaluation domain - to collect data, analyse risk and maintain a risk profile and the risk response domain - to articulate risk, manage risk, react to events) as illustrated in Figure 5.5 below.

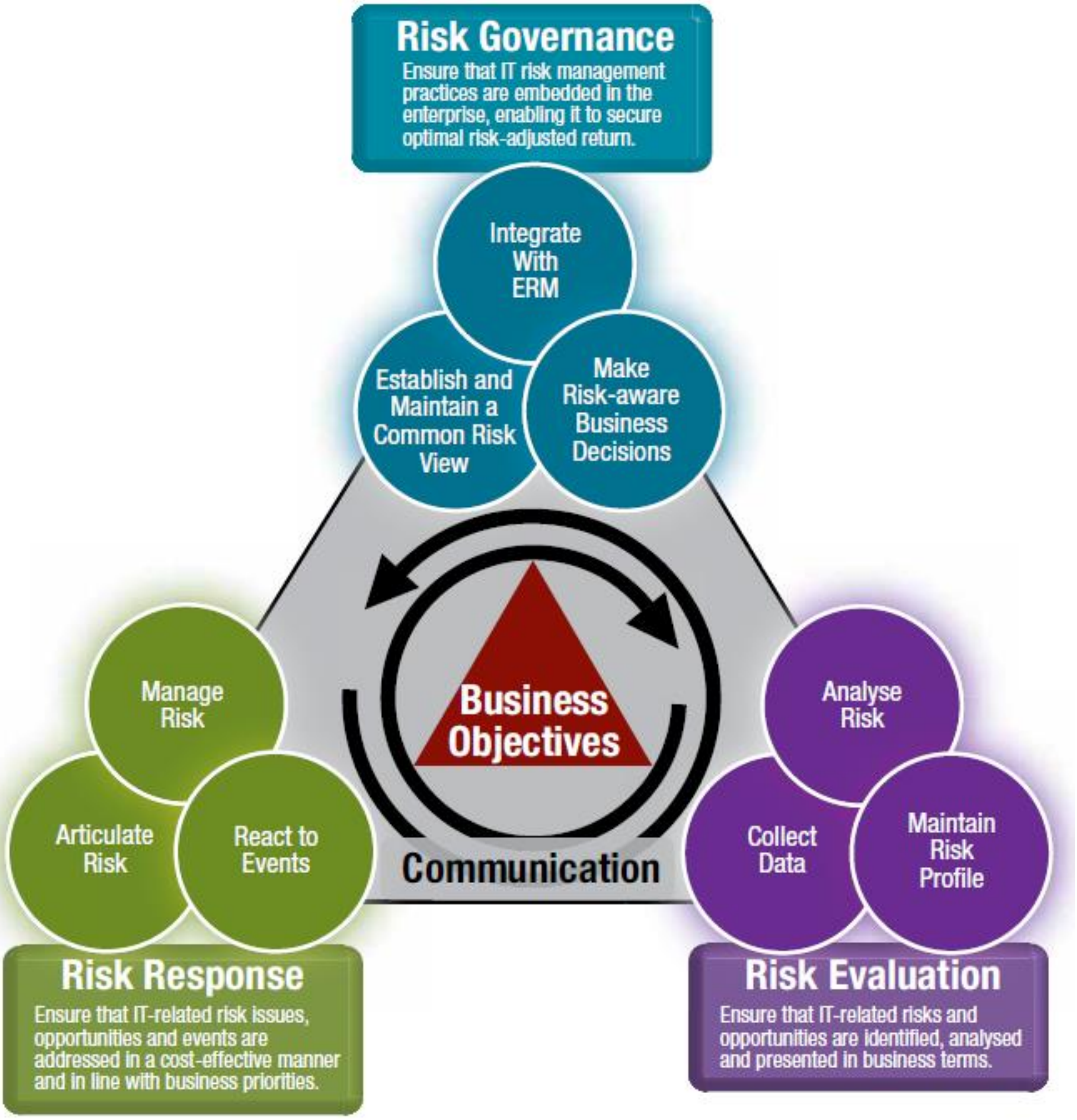

Risk Governance
Ensure that IT risk management practices are embedded in the enterprise, enabling it to secure optimal risk-adjusted return.
Integrate With ERM
Establish and Maintain a Common Risk View
Make Risk-aware Business Decisions
Business Objectives
Communication
Manage Risk
Articulate Risk
React to Events
Risk Response
Ensure that IT-related risk issues, opportunities and events are addressed in a cost-effective manner and in line with business priorities.
Analyse Risk
Collect Data
Maintain Risk Profile
Risk Evaluation
Ensure that IT-related risks and opportunities are identified, analysed and presented in business terms.

Figure 5.5: Risk IT Framework

Source: ISACA (2009)

5.5.2.2.2 National Institute of Standards and Technology (NIST)

The NIST in the United States of America (USA) develops information security standards, guidelines and specifies the minimum requirements for federal information systems (2013). As a result, the NIST Special Publication 800-53 (2013) provides guidelines for selecting and specifying security controls to meet the Minimum Security Requirements for Federal Information and Information Systems as required by the Federal Information Processing Standards (FIPS).

Revision 3 of the NIST Special Publication 800-53 was released in August 2009 (NIST, 2009) and this was followed by Revision 4 (NIST, 2013), which was released in April 2013. The NIST Special Publication 800-53 (2013) groups security controls into 18 families as illustrated in Table 5.2 below.

Table 5.2: NIST 18 Families of Security Controls

Source: Adapted from NIST (2013)

Number	Security control family ID	Security control family name
1	AC	Access Control
2	AT	Awareness and Training
3	AU	Audit and Accountability
4	CA	Security Assessment and Authorization
5	CM	Configuration Management
6	CP	Contingency Planning
7	IA	Identification and Authentication
8	IR	Incident Response
9	MA	Maintenance
10	MP	Media Protection
11	PE	Physical and Environmental Protection
12	PL	Planning
13	PS	Personnel Security
14	RA	Risk Assessment
15	SA	System and Services Acquisition

Number	Security control family ID	Security control family name
16	SC	System and Communications Protection
17	SI	System and Information Integrity
18	PM	Program Management

Each of the 18 families of security controls listed in Table 5.2 above consists of the related security controls, for example, the Audit and Accountability family includes 16 security controls as illustrated in Table 5.3 below.

Table 5.3: Security Controls from the Audit and Accountability Family

Source: Adapted from NIST (2013)

Security control family		Audit and Accountability
Number	**Security control ID**	**Security control name**
1	AU-1	Audit and Accountability Policy and Procedures
2	AU-2	Audit Events
3	AU-3	Content of Audit Records
4	AU-4	Audit Storage Capacity
5	AU-5	Response to Audit Processing Failures
6	AU-6	Audit Review, Analysis, and Reporting
7	AU-7	Audit Reduction and Report Generation
8	AU-8	Time Stamps
9	AU-9	Protection of Audit Information
10	AU-10	Non-Repudiation
11	AU-11	Audit Record Retention
12	AU-12	Audit Generation
13	AU-13	Monitoring for Information Disclosure
14	AU-14	Session Audit
15	AU-15	Alternate Audit Capability
16	AU-16	Cross-Organisational Auditing

5.5.2.2.3 Office of Government Commerce United Kingdom (OGCUK)

The OGCUK developed the Information Technology Infrastructure Library (ITIL) framework as an approach to IT service management (OGCUK, 2007a). This framework is currently in its third revision which was released in 2007 and addresses service lifecycle governance processes which is comprised of continual service improvement and service strategy processes, while service lifecycle operational processes is comprised of service design, service transition and service operation processes as illustrated in Figure 5.6 below (OGCUK, 2007a). In addition, each of the aforementioned components are supported by underlining processes, for example as illustrated in Figure 5.6, service strategy processes are supported by demand management, strategy generation, service portfolio management and information technology financial management processes.

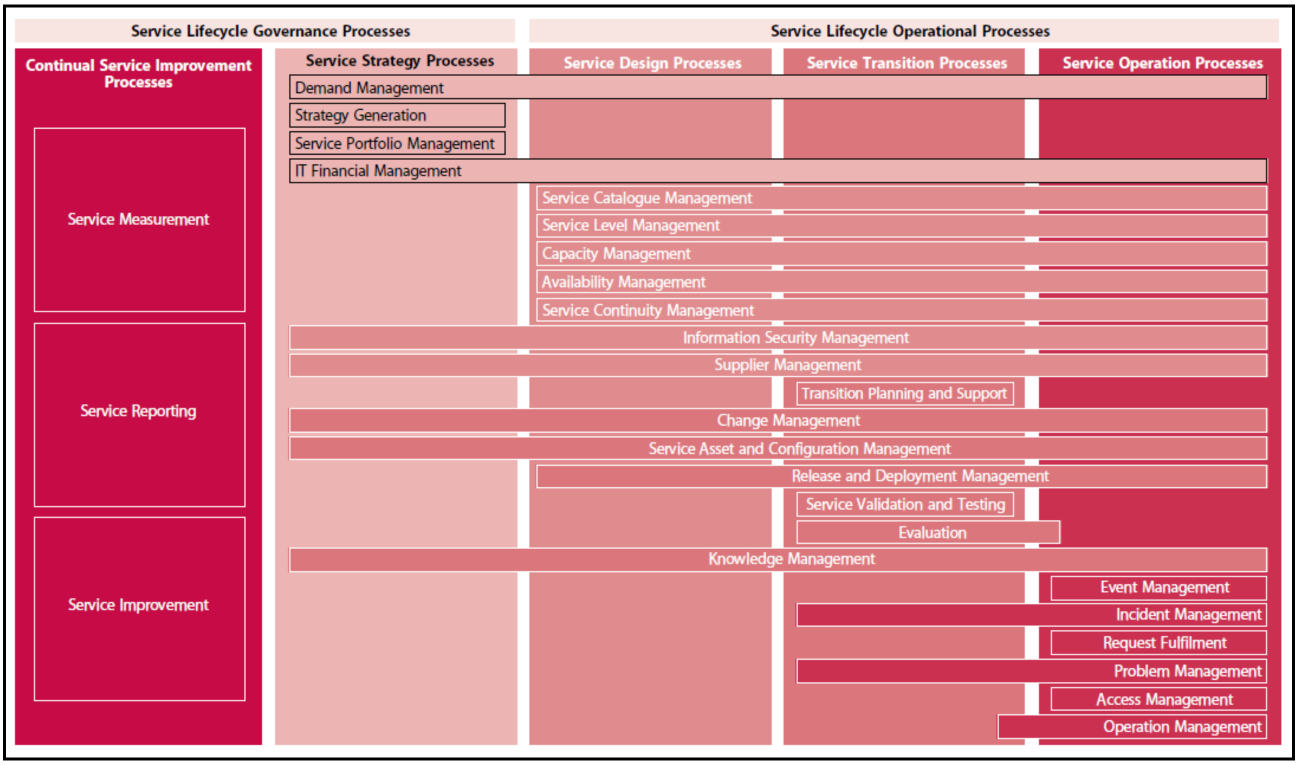

Service Lifecycle Governance Processes
Service Lifecycle Operational Processes
Continual Service Improvement Processes
Service Strategy Processes
Service Design Processes
Service Transition Processes
Service Operation Processes
Demand Management
Strategy Generation
Service Portfolio Management
IT Financial Management
Service Measurement
Service Catalogue Management
Service Level Management
Capacity Management
Availability Management
Service Continuity Management
Information Security Management
Supplier Management
Service Reporting
Transition Planning and Support
Change Management
Service Asset and Configuration Management
Release and Deployment Management
Service Validation and Testing
Evaluation
Knowledge Management
Service Improvement
Event Management
Incident Management
Request Fulfilment
Problem Management
Access Management
Operation Management

Figure 5.6: Information Technology Infrastructure Library (ITIL) Framework

Source: OGCUK (2007a)

5.5.2.2.4 International Organisation for Standardisation (ISO)

The International Organisation for Standardisation (ISO) in 2005 developed an Information Security Management System (ISMS) standard, ISO 27001 (BSI, 2005). In 2005, the ISO 27001 standard consisted of 133 controls across 11 groups (BSI, 2005). The latest revision to the ISO 27001 standard in 2013 consists of 14 groups, as illustrated in Table 5.4 below, which in turn comprise of 114 controls (ISO, 2013). For example, the Human Resource Security group within the ISO 27001 standard (ISO, 2013) consists of controls relating to prior employment (screening, terms and conditions of employment), during employment (management responsibilities, information security awareness, education and training as well as disciplinary process) as well as termination and change of employment (termination or change of employment responsibilities) controls.

Table 5.4: ISO 27001 - 14 Groups of Security Controls

Source: Adapted from ISO (2013)

Number	**Security group control ID**	**Security group name (number of controls)**
1	A.5	Information Security Policies (2 Controls)
2	A.6	Organisation of Information Security (7 Controls)
3	A.7	Human Resource Security (6 Controls)
4	A.8	Asset Management (10 Controls)
5	A.9	Access Control (14 Controls)
6	A.10	Cryptography (2 Controls)
7	A.11	Physical and Environmental Security (15 Controls)
8	A.12	Operations Security (14 Controls)
9	A.13	Communications Security (7 Controls)
10	A.14	System Acquisition, Development and Maintenance (13 Controls)
11	A.15	Supplier Relationships (5 Controls)
12	A.16	Information Security Incident Management (7 Controls)
13	A.17	Information Security Aspects of Business Continuity Management (4 Controls)

Number	Security group control ID	Security group name (number of controls)
14	A.18	Compliance (8 Controls)

Similarly in 2012, the ISO developed a business continuity management standard, ISO 22301 to assist institutions with the establishment, implementation, operation, monitoring, review, maintenance and improvement of business continuity capabilities in order to ensure continued operations in the event of a disruption (ISO, 2012). Furthermore, ISO 22301 specifies the requirements for setting up and managing a business continuity management system in 7 sections - context, leadership, planning, support, operation, evaluation and improvement (ISO, 2012).

5.5.2.3 Specific Selection of Security Safeguards

The security safeguards which form part of the "Secure" phase of the proposed POPI Condition 7 framework is not the selection and implementation of leading practices mentioned above such as COBIT (ISACA, 2014c) Risk IT (ISACA, 2009), NIST Special Publication 800-53 (NIST, 2009 and 2013), ITIL (OGCUK, 2007a and 2007b), ISO 27001 (BSI, 2005 and ISO, 2013) or ISO 2230 (Drewitt, 2013 and ISO, 2012) in its entirety. The security safeguards which form part of the "Secure" phase of the proposed POPI Condition 7 framework is instead a specific selection of security safeguards prescribed by the various leading practices as a means to address a specific requirement, which in this case is to ensure the confidentiality and integrity of electronic personal information and in so doing to achieve and maintain compliance with Condition 7 of the POPI Act (2013).

NIST classifies security safeguards into 3 domains (2009). The first domain is the management domain, which focuses on managing risk by key stakeholders providing direction and intent to the protection of personal information initiative (NIST, 2009). The operational domain is the second domain, which focuses on people executing processes associated with managing and monitoring security safeguards (NIST, 2009). The third domain is the technical domain, which focuses on the implementation and execution of security safeguards driven by technology (NIST, 2009). As a result, the management, operational and technical domains form the basis of the "Secure" phase of the proposed POPI Condition 7 framework in that a selection of security safeguards are specifically proposed for each of the 3 domains as illustrated in Figure 5.7 below.

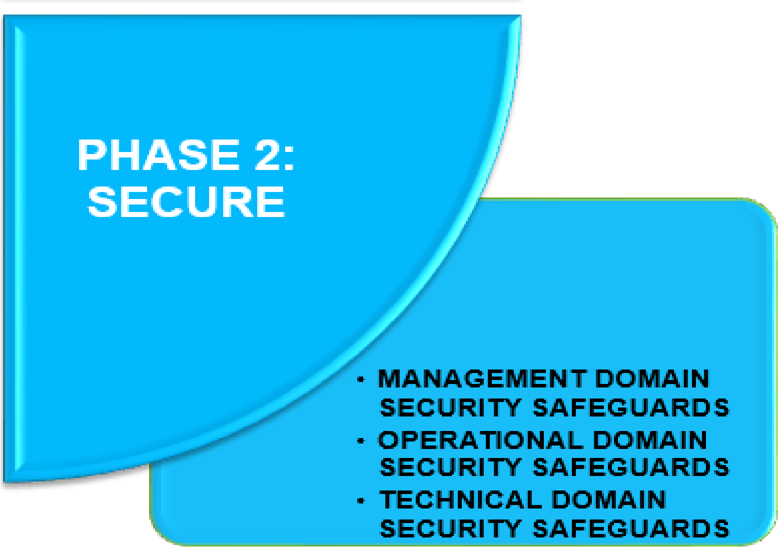

PHASE 2:
SECURE
• MANAGEMENT DOMAIN SECURITY SAFEGUARDS
• OPERATIONAL DOMAIN SECURITY SAFEGUARDS
• TECHNICAL DOMAIN SECURITY SAFEGUARDS

Figure 5.7: Proposed POPI Condition 7 Framework - Phase 2 (Secure)

5.5.2.3.1 Management Domain Security Safeguards

As such, the management domain of the "Secure" phase consists of 5 security safeguards as illustrated in Figure 5.8 below.

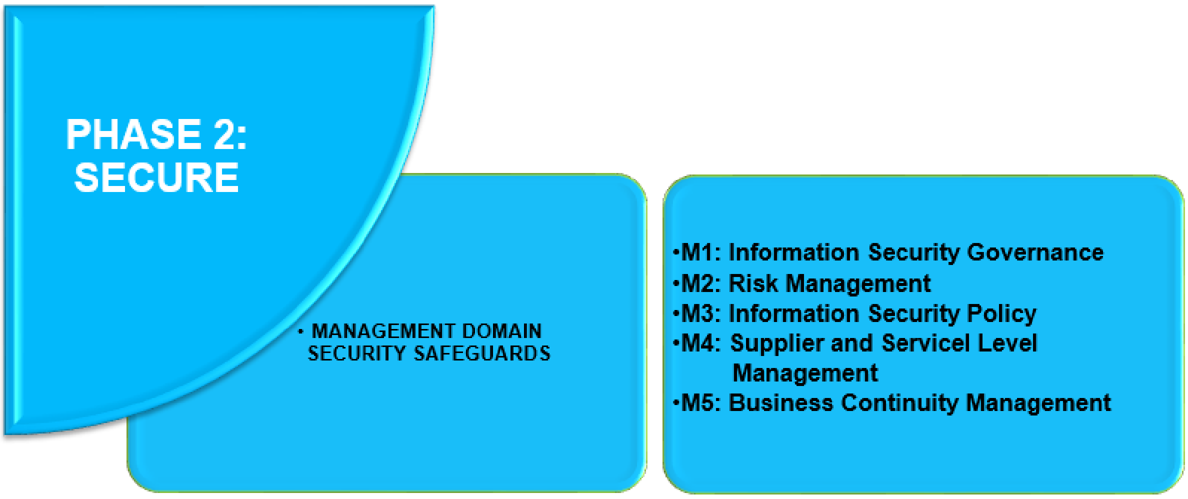

PHASE 2:
SECURE
• MANAGEMENT DOMAIN SECURITY SAFEGUARDS
•M1: Information Security Governance
•M2: Risk Management
•M3: Information Security Policy
•M4: Supplier and Servicel Level Management
•M5: Business Continuity Management

Figure 5.8: Secure Phase - Management Domain (5 Security Safeguards)

The first safeguard within the management domain is *M1: Information Security Governance*. This security safeguard is an integral part of governance that encompasses leadership, organisational structures as well as clear roles and responsibilities (ISACA, 2006 and ISO, 2013) for safeguarding electronic personal information. *M2: Risk Management* is the second safeguard within the management domain and requires the governance, evaluation and a response to risks presented by electronic personal information (ISACA, 2009 and 2014c). The third safeguard, *M3: Information Security Policy*, requires management direction and support for information security to be achieved through a formally defined and approved information security policy (ISO, 2013). *M4: Supplier and Service Level Management* is the fourth safeguard of the management domain which focuses on the contracts in place with third party operators external to the institution as well as internal stakeholders within the institution responsible for providing services in relation to electronic personal information (ISACA, 2014c and OGCUK, 2007a). Lastly, the *M5: Business Continuity Management* safeguard addresses the ability to recover from a business interruption in the most effective and efficient manner (Drewitt, 2013, ISACA, 2014c, ISO 2012 and 2013), which includes the recovery of electronic personal information maintained by an institution.

5.5.2.3.2 OPERATIONAL DOMAIN SECURITY SAFEGUARDS

The operational domain of the "Secure" phase consists of 6 security safeguards as illustrated in Figure 5.9 below.

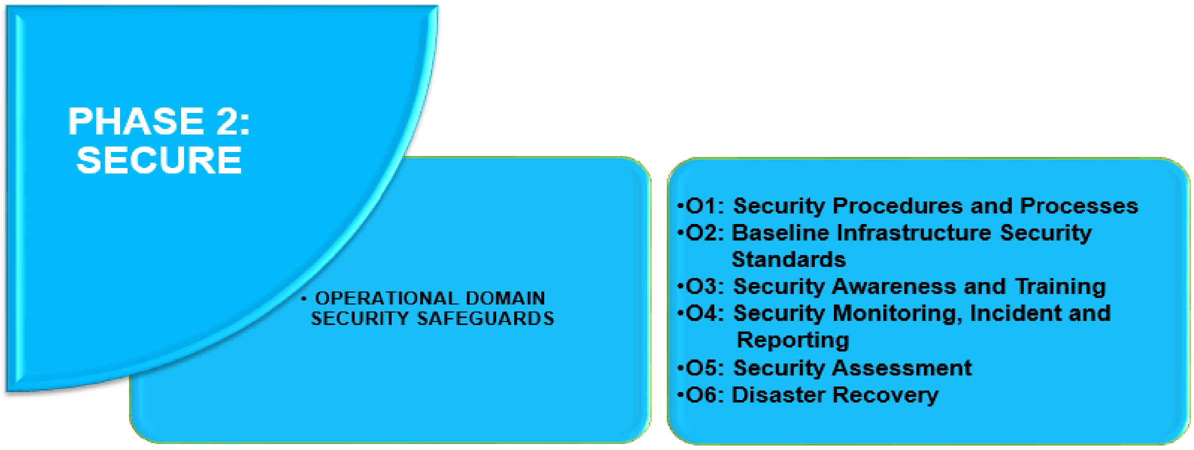

PHASE 2: SECURE
• OPERATIONAL DOMAIN SECURITY SAFEGUARDS
•O1: Security Procedures and Processes
•O2: Baseline Infrastructure Security Standards
•O3: Security Awareness and Training
•O4: Security Monitoring, Incident and Reporting
•O5: Security Assessment
•O6: Disaster Recovery

Figure 5.9: Secure Phase - Operational Domain (6 Security Safeguards)

The first security safeguard in the operational domain is *O1: Security Procedures and Processes.* This security safeguard addresses the security procedures and processes in place to maintain confidentiality and integrity of electronic personal information. The security procedure and process areas to be considered include: change and configuration management, patch management, availability management, incident management, backup management, user account and access management (ISACA, 2014c, ISO, 2013 and OGCUK, 2007b) as well as the management of encryption keys to secure data channels (BSI, 2005). *O2: Baseline Infrastructure Security Standards* is the second safeguard in the operational domain and focuses on all server, workstation and laptop operating systems, database servers, web servers, network components (firewalls, routers, wireless) that form part of the technology infrastructure, to enable the protection of electronic personal information, baseline infrastructure security standards should be applied as a security safeguard to prevent the adoption of default configurations and to ensure consistent configurations (NIST, 2013). The third security safeguard in this domain is *O3: Security Awareness and Training* which focuses on employees, contractors or third party operators need to be provided with awareness and training with regards to information security (ISO, 2013, NIST, 2013 and OGCUK, 2007b), with a specific focus on the security of electronic personal information. *O4: Security Monitoring, Incident and Reporting* is the fourth security safeguard in the operational domain that requires all audit logs from applications as well as the technology infrastructure to be assessed in order to report on any malicious activities or data breaches of electronic personal information (ISACA, 2014c, NIST, 2013 and OGCUK, 2007b). Furthermore, the incident management processes may report a data breach of electronic personal information. The fifth security safeguard in this domain is *O5: Security Assessment* requiring regular security assessments to be performed in order to assess the security posture of the institution from a technical, organisational, procedural, administrative or physical security perspective (NIST, 2013 and Palmer et al., 2001). The last security safeguard in the operational domain is *O6: Disaster Recovery* which requires people, processes and technology associated with the storage, processing and transmission of electronic personal information as well as to ensure continued operations to be defined (Drewitt, 2013, ISO 2012 and 2013, and NIST 2013).

5.5.2.3.3 Technical Domain Security Safeguards

Lastly, the technical domain of the "Secure" phase consists of 9 security safeguards as illustrated in Figure 5.10 below.

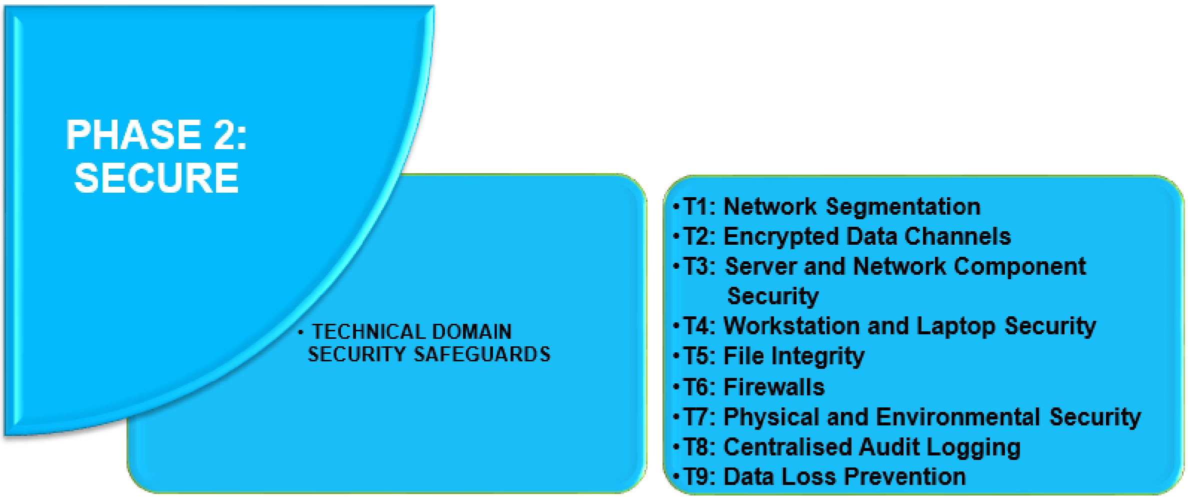

PHASE 2:
SECURE
• TECHNICAL DOMAIN SECURITY SAFEGUARDS
•T1: Network Segmentation
•T2: Encrypted Data Channels
•T3: Server and Network Component Security
•T4: Workstation and Laptop Security
•T5: File Integrity
•T6: Firewalls
•T7: Physical and Environmental Security
•T8: Centralised Audit Logging
•T9: Data Loss Prevention

Figure 5.10: Secure Phase - Technical Domain (9 Security Safeguards)

T1: Network Segmentation is the first security safeguard in the technical domain. The segmentation of a network entails a logical grouping of related network assets, resources and applications (Solomon, 2011). As a result, all the application and database servers that respectively process and store personal information should be located on a dedicated network segment that is separated from the rest of the corporate network (NIST, 2013). The second security safeguard in this domain is *T2: Encrypted Data Channels* requiring all electronic personal information flowing into and out of the dedicated network segment to be encrypted and access to the data channels should be strictly monitored and controlled (ISO, 2013 and NIST, 2013). *T3: Server and Network Component Security* is the third security safeguard in this domain which specifies that all server and network components should be configured to implement the defined baseline infrastructure security standards, *O2 - Baseline infrastructure security standards*, adopted in the operational domain (ISACA, 2014c and NIST, 2013). The fourth security safeguard in the technical domain is *T4: Workstation and Laptop Security* which requires all workstations and laptops to be configured as per the defined baseline infrastructure security standards adopted and be locked down to prevent the user to change the configuration or install additional applications not authorised by the institution (ISACA, 2014c and NIST, 2013). *T5: File Integrity* is the fifth security safeguard in this domain and requires all configurations associated with server and network components to be associated with a unique value known as a hash value. The hash value may be used to ascertain if unauthorised changes were affected to configurations (ISACA, 2014c and OGCUK, 2007b). The sixth security safeguard in this domain is *T6: Firewalls* used to separate networks by controlling access and analysing traffic between networks (ISACA, 2013). As such a firewall should be used to separate the application and database servers that respectively process and store electronic personal information located on a dedicated network segment from the rest of the corporate network (NIST, 2013). *T7: Physical and Environmental Security* is the seventh security safeguard in this domain requiring physical and environmental security safeguards in place within the server rooms hosting the applications as well as the technology infrastructure associated with the storage, processing and transmission of electronic personal information. Physical security safeguards to control access to the server rooms and environmental security safeguards to provide alternate power sources to ensure availability as well as to protect against environmental hazards such as floods and fire should be in place (ISACA, 2014c, ISO, 2013 and NIST, 2013). The eight security safeguard in this domain is *T8: Centralised audit logging* which requires audit logs to be maintained for all applications as well as the technology infrastructure associated with storing, processing and transmitting electronic personal information. All the audit logs maintained should be sent to a centralised audit logging server where analysis may be performed to identify ineffective security safeguards as well as security incidents and to serve as the basis for conducting an investigation in the event of a data breach of electronic personal information (ISACA, 2014c, ISO, 2013 and NIST, 2013). Lastly, the ninth security safeguard within the technical domain is *T9: Data loss prevention*, which entails the protection of data loss for data at rest, in motion or at an end point (Kanagasingham, 2008). As such, to prevent the loss of electronic personal information specifically via workstations or laptops utilised by users to access applications processing personal information or databases storing personal information, data loss prevention should be implemented (ISACA, 2014c, ISO, 2012 and NIST, 2013).

5.5.2.4 SUMMARY AND SOURCE OF THE SPECIFIC SELECTION OF SECURITY SAFEGUARDS

Table 5.5 below provides a summary of the specific selection of security safeguards as part of the "Secure" phase of the proposed POPI Condition 7 framework across the management, operational and technical domains. In addition, Table 5.5 provides the source of the security safeguards to ensure the confidentiality and integrity of electronic personal information identified in Phase 1 ("Identify"). For example, the *M2: Risk Management* security safeguard of the proposed POPI Condition 7 framework falls within the management domain and the source of the security safeguard are the COBIT and Risk IT leading practices developed by ISACA.

Table 5.5: Summary and Source of the Specific Selection of Security Safeguards

Selected security safeguard	**ISACA**	**NIST**	**OGCUK**	**ISO**
Management domain				
M1: Information Security Governance	COBIT			ISO 27001
M2: Risk Management	COBIT RISK IT			
M3: Information Security Policy				ISO 27001
M4: Supplier and Service Level Management	COBIT		ITIL	
M5: Business Continuity Management	COBIT			ISO 22301 ISO 27001
Operational domain				
O1: Security Procedures and Processes	COBIT		ITIL	ISO 27001
O2: Baseline Infrastructure Security Standards		NIST Special		

Selected security safeguard	**ISACA**	**NIST**	**OGCUK**	**ISO**
		Publication 800-53		
O3: Security Awareness and Training		NIST Special Publication 800-53	ITIL	ISO 27001
O4: Security Monitoring, Incident and Reporting	COBIT	NIST Special Publication 800-53	ITIL	
O5: Security Assessment		NIST Special Publication 800-53		
O6: Disaster Recovery		NIST Special Publication 800-53		ISO 22301 ISO 27001
Technical domain				
T1: Network Segmentation		NIST Special Publication 800-53		
T2: Encrypted Data Channels		NIST Special Publication 800-53		ISO 27001
T3: Server and Network Component Security	COBIT	NIST Special		

Selected security safeguard	ISACA	NIST	OGCUK	ISO
		Publication 800-53		
T4: Workstation and Laptop Security	COBIT	NIST Special Publication 800-53		
T5: File Integrity	COBIT		ITIL	
T6: Firewalls		NIST Special Publication 800-53		
T7: Physical and Environmental Security	COBIT	NIST Special Publication 800-53		ISO 27001
T8: Centralised Audit Logging	COBIT	NIST Special Publication 800-53		ISO 27001
T9: Data Loss Prevention	COBIT	NIST Special Publication 800-53		ISO 22301

The “Secure” phase of the proposed POPI Condition 7 framework is followed by the “Monitor and Report” phase.

5.5.3 Phase 3: Monitor and Report

Phase 3, “Monitor and Report”, consists of 2 aspects namely, monitoring and reporting as illustrated in Figure 5.11 on the next page. This phase ensures that the electronic personal information remains protected and instances when the protection is not in place this should be reported in order to initiate remedial action.

PHASE 3: MONITOR AND REPORT
• MONITORING SECURITY SAFEGUARDS
• REPORTING ON SECURITY SAFEGUARDS

Figure 5.11: Proposed POPI Condition 7 Framework - Phase 3 (Monitor and Report)

The 2 aspects of this phase namely, “Monitor” and “Report” as illustrated in Figure 5.11 above are unpacked below in subsection 5.5.3.1 and 5.5.3.2 respectively.

5.5.3.1 Monitor Aspect

The “Monitor” aspect of this phase is dependent on the *O4: Security Monitoring, Incident and Reporting* security safeguard, which forms part of the operational domain (O4) of the “Secure” phase. As such, the “Monitor” aspect of this phase addresses the monitoring of the selection of security safeguards in the operational and technical domains implemented in the “Secure” phase of the proposed POPI Condition 7 framework to ensure that the implemented security safeguards are working as intended.

5.5.3.2 Report Aspect

The “Report” aspect of this phase addresses reporting in terms of the effectiveness of the implemented security safeguards. In the event of a security compromise of electronic personal information, specific information regarding the compromise, such as the security safeguard that was circumvented and the nature and extent of electronic personal information disclosed or modified, may be required. Furthermore, an inspection of the audit logs maintained on the centralised audit logging server, as required by *T8: Centralised Audit Logging*, may potentially provide information of how and by whom the security compromise was performed. All information gathered relating to the security compromise will need to be availed to internal stakeholders for further investigation as well as to the external Information Regulator to ensure compliance with Section 22 of Condition 7 (notification in the event of a security compromise of personal information) of the POPI Act (2013).

The "Monitor and Report" phase of the proposed POPI Condition 7 framework is followed by the final phase known as the "Remediate" phase.

5.5.4 PHASE 4: REMEDIATE

The final phase, "Remediate", as illustrated in Figure 5.12 below, addresses remedial action in the form of correction of security safeguards in place or the implementation of adequate security safeguards to ensure that the protection of electronic personal information is maintained.

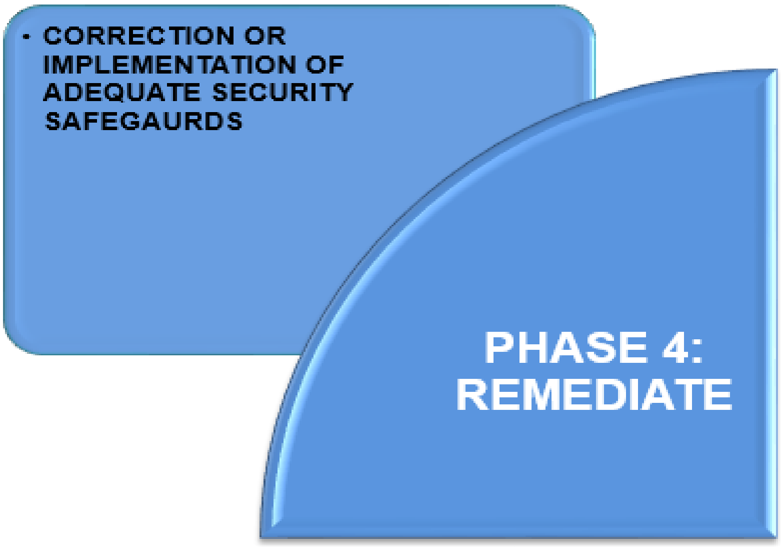

• CORRECTION OR IMPLEMENTATION OF ADEQUATE SECURITY SAFEGAURDS
PHASE 4: REMEDIATE

Figure 5.12: Proposed POPI Condition 7 Framework - Phase 4 (Remediate)

The correction of security safeguards in place or the implementation of adequate security safeguards as illustrated in Figure 5.12 on the previous page is unpacked below in subsection 5.5.4.1.

5.5.4.1 Correction or Implementation of Adequate Security Safeguards

During the “Monitor” aspect of Phase 3 of the proposed POPI Condition 7 framework, if it is identified that a security safeguard is not working as intended or a security compromise has occurred resulting in a circumvented security safeguard, immediate action should be taken as electronic personal information may be disclosed or modified, resulting in the compromise of electronic personal information. This compromise may negatively impact an institution from a compliance, financial and reputational perspective. As a result, the “Remediate” phase is aimed to correct the current security safeguard or implement an alternate adequate security safeguard to maintain the confidentiality and integrity of electronic personal information and to ultimately ensure compliance with Section 19 of Condition 7 of the POPI Act (2013).

The proposed POPI Condition 7 framework through the 4 aforementioned phases clearly demonstrates an approach, which includes a specific selection of security safeguards as part of the “Secure” phase, to ultimately address the requirements of Condition 7 of the POPI Act (2013), specifically in relation to electronic personal information. The section which follows provides a critical evaluation of the proposed POPI Condition 7.

5.6 Critical Evaluation - Benefits and Limitations

A critical evaluation of the proposed POPI Condition 7 framework led to the identification of benefits and limitations associated with the proposed POPI Condition 7 framework.

A major benefit of the proposed POPI Condition 7 framework is that it provides South African institutions with a 4-phased (“Identify”, “Secure”, “Monitor and Report” and “Remediate”) approach to ultimately address the requirements of Condition 7 of the POPI Act (2013), specifically in relation to electronic personal information, as illustrated in Table 5.6 on the next page.

Table 5.6: Condition 7 Requirements of the POPI Act Addressed by the Proposed POPI Condition 7 Framework

Condition 7 section number	Condition 7 requirement	Condition 7 requirement addressed by the proposed POPI Condition 7 framework
19	The need to implement security safeguards to ensure the confidentiality and integrity of personal information.	Phase 2 - "Secure” Phase 4 - “Remediate"
20	The responsibilities for handling personal information.	Phase 1 - "Identify”
21	The responsibilities of an operator processing personal information.	Phase 1 - "Identify”
22	The need for notification in the event of a security compromise of personal information.	Phase 3 - "Monitor and Report” Phase 4 - “Remediate"

According to Monty (2015), the POPI Act (2013) requires reasonable measures to be taken to protect personal information in order to reduce the risk of potential data breaches and the associated public relations and legal ramifications for an institution. As such, another benefit associated with the proposed POPI Condition 7 framework is that the “Secure” phase provides South African institutions with specific guidance in terms of the reasonable measures, in the form of security safeguards, to consider for ensuring the confidentiality and integrity of electronic personal information required to ultimately achieve and maintain compliance with Condition 7 of the POPI Act (2013).

The proposed POPI Condition 7 framework may be applied within any institution in the public or private sector, independent of the institution size or industry sector that is required to ensure the confidentiality and integrity of electronic personal information required to ultimately achieve and maintain compliance with Condition 7 of the POPI Act (2013).

The "Identify", "Monitor and Report", and "Remediate" phases of the proposed POPI Condition 7 framework may be applied to personal information in both electronic format (within information systems and their corresponding databases) and non-electronic format (hard copy or paper based outside information systems). In addition, the security safeguards in the management and operational domains of the "Secure" phase may be applied to personal information in both electronic and non-electronic format.

Another benefit associated with the proposed POPI Condition 7 framework is that a summary of the source in terms of leading practices is provided for in the selection of security safeguards within the "Secure" phase to ensure the confidentiality and integrity of electronic personal information, as illustrated in Table 5.5 within section 5.5.2.4. This serves as a point of reference for further detailed guidance relating to the proposed security safeguards. For example, when addressing the disaster recovery security safeguard (O6 in Table 5.5 above within section 5.5.2.4), ISO 22301 and ISO 27001 as well as the NIST Special Publication 800-53 leading practices may provide the further guidance required. In addition, if an institution has for example implemented the COBIT leading practice, the source of the selection of security safeguards as listed in Table 5.5 above within section 5.5.2.4 may be used to assess the gap in terms of the security safeguards already in place as a result of implementing COBIT (such as *M1: Information Security Governance*, *M2: Risk Management* and *O4: Security Monitoring, Incident and Reporting*) and the security safeguards that still need to be implemented (*M3: Information Security Policy* or *T2: Encrypted Data Channels*). In addition, the source of the selection of security safeguards as listed in Table 5.5 above within section 5.5.2.4 may be used to explore appropriate leading practices in order to implement outstanding security safeguards, for example in terms of the *T6: Firewalls* security safeguard the NIST Special Publication 800-53 may be explored.

Lastly, from a benefit perspective the proposed POPI Condition 7 framework is not the selection and implementation of leading practices such as COBIT (ISACA, 2014c) RISK IT (ISACA, 2009), NIST Special Publication 800-53 (NIST, 2009 and 2013), ITIL (OGCUK, 2007a and 2007b), ISO 27001 (BSI, 2005 and ISO, 2013) or ISO 2230 (Drewitt, 2013 and

ISO, 2012) in its entirety. However, the proposed POPI Condition 7 framework is instead a specific selection of security safeguards prescribed by the various leading practices as a means to address a specific requirement, which in this case is to achieve compliance with Condition 7 of the POPI Act (2013) in relation to electronic personal information.

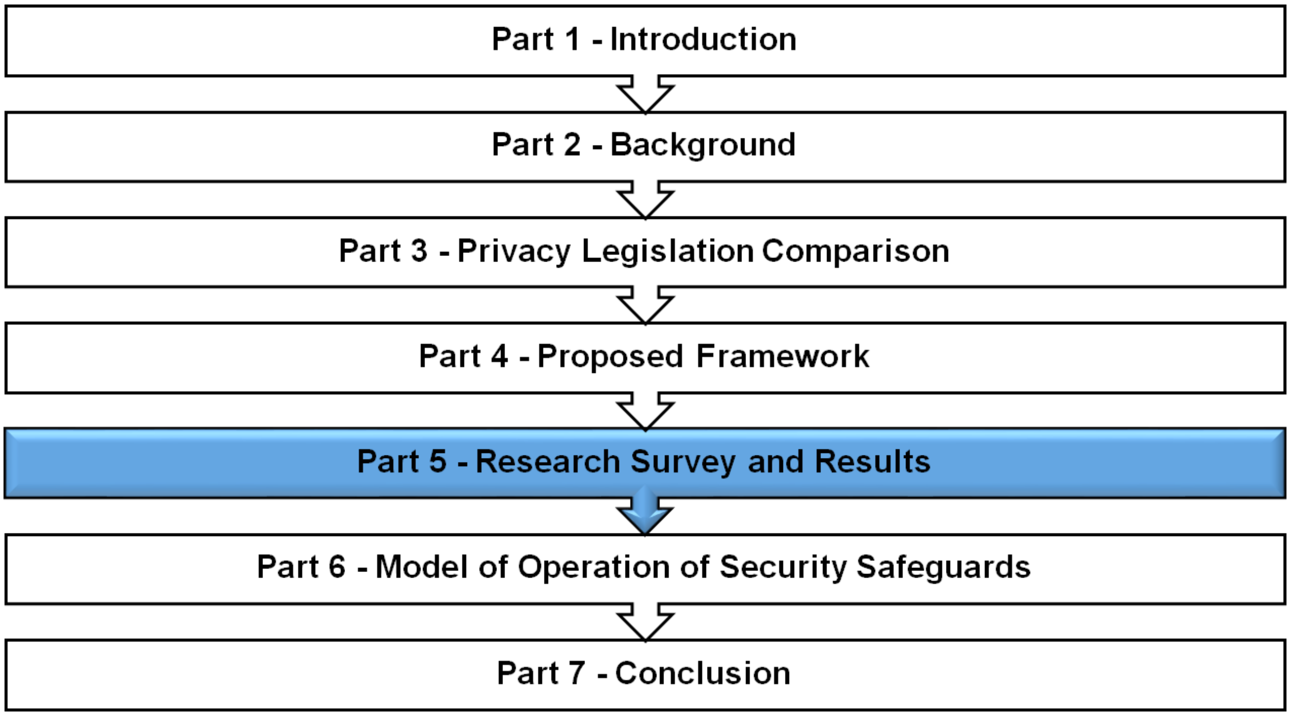
A limitation of the proposed POPI Condition 7 framework is that the security safeguards in the technical domain of the “Secure” phase is focused on the personal information stored, processed and transmitted in electronic format as opposed to non-electronic format. Furthermore, the proposed POPI Condition 7 framework is limited to addressing only the requirements of Condition 7 of the POPI Act (2013) in relation to electronic personal information.

5.7 Conclusion

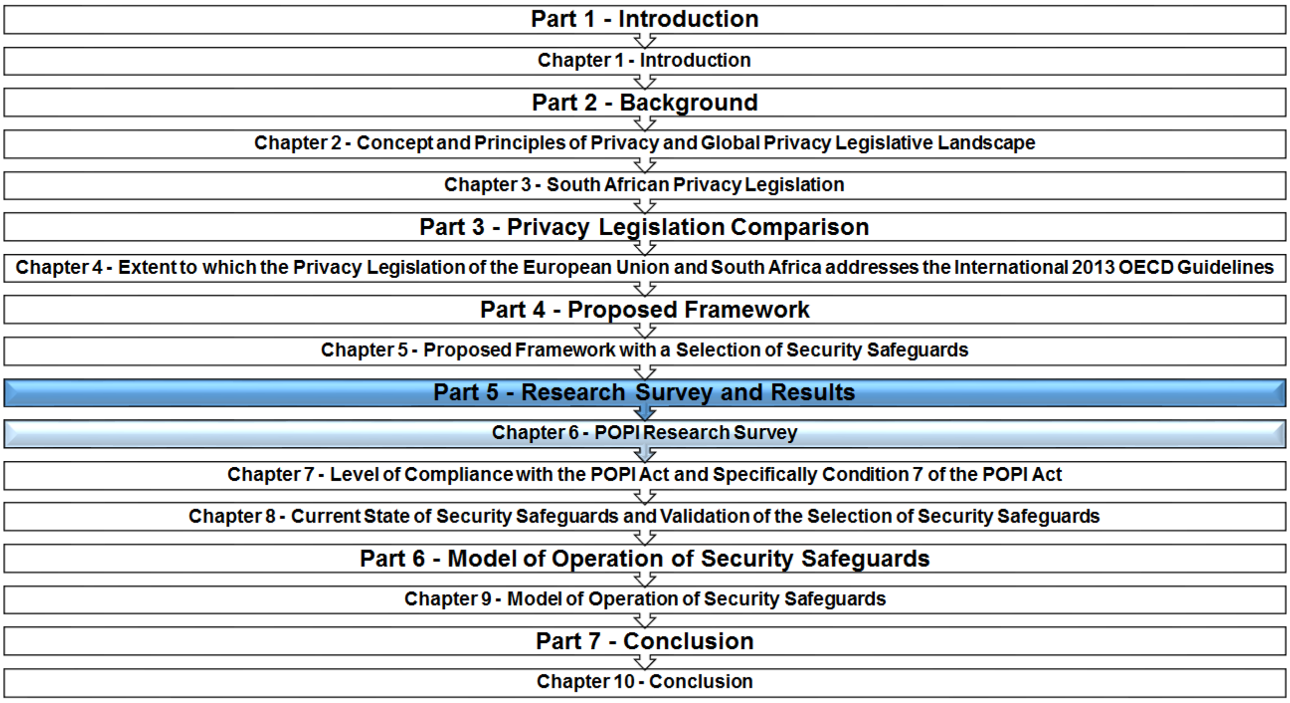
This chapter concluded Part 4 (Proposed Framework) of this thesis by outlining the requirements of Condition 7 of the POPI Act (2013) and then addressed the research question associated with this chapter by proposing the POPI Condition 7 framework to ultimately address the requirements of Condition 7 of the POPI Act (2013), specifically in relation to electronic personal information. The proposed POPI Condition 7 framework consisted of a 4-phased (“Identify”, “Secure”, “Monitor and Report” and “Remediate”) approach, which encapsulates a specific selection of 20 security safeguards across 3 domains (management, operational and technical) as part of the “Secure” phase to ensure confidentiality and integrity of electronic personal information stored, processed or transmitted. Lastly, a critical evaluation in terms of the benefits and limitations associated with the proposed POPI Condition 7 framework was provided.

Part 5 (Research Survey and Results) of this thesis follows this chapter and is comprised of Chapter 6, 7 and 8 respectively. Chapter 6 which follows provides an overview of the POPI research survey used to address the research questions associated with Chapter 7 and 8 of this thesis.

PART 5 - RESEARCH SURVEY AND RESULTS


Part 1 - Introduction
Part 2 - Background
Part 3 - Privacy Legislation Comparison
Part 4 - Proposed Framework
Part 5 - Research Survey and Results
Part 6 - Model of Operation of Security Safeguards
Part 7 - Conclusion

CHAPTER 6 - POPI RESEARCH SURVEY



Part 1 - Introduction

Chapter 1 - Introduction

Part 2 - Background

Chapter 2 - Concept and Principles of Privacy and Global Privacy Legislative Landscape

Chapter 3 - South African Privacy Legislation

Part 3 - Privacy Legislation Comparison

Chapter 4 - Extent to which the Privacy Legislation of the European Union and South Africa addresses the International 2013 OECD Guidelines

Part 4 - Proposed Framework

Chapter 5 - Proposed Framework with a Selection of Security Safeguards

Part 5 - Research Survey and Results

Chapter 6 - POPI Research Survey

Chapter 7 - Level of Compliance with the POPI Act and Specifically Condition 7 of the POPI Act

Chapter 8 - Current State of Security Safeguards and Validation of the Selection of Security Safeguards

Part 6 - Model of Operation of Security Safeguards

Chapter 9 - Model of Operation of Security Safeguards

Part 7 - Conclusion

Chapter 10 - Conclusion

6.1 INTRODUCTION

A framework to achieve and maintain compliance with Condition 7 of the Protection of Personal Information (POPI) Act (Act 4 of 2013) was proposed in Chapter 5. The proposed POPI Condition 7 framework included a selection of security safeguards to ensure the confidentiality and integrity of electronic personal information stored, processed or transmitted. This chapter provides an overview of the POPI research survey used to address research question 3 covered in Chapter 7, as well as research questions 4 and 5 covered in Chapter 8.

The overview of the POPI research survey includes the research design, research instrumentation, research group, data analysis approach and the POPI research survey results in terms of demographics, as it relates to the participants' institutions' sector (public versus private), industry sector and institution size.

6.2 RESEARCH DESIGN

Research may be descriptive, casual or exploratory in nature (Anusree et al., 2014). Descriptive research is pre-planned, aimed at observations based on characteristics and is more quantitative in nature by focusing on collecting data that can be inferred from a population (Anusree et al., 2014). Casual research is similar to descriptive research in that it is pre-planned and more quantitative in nature but differs in that is focuses on the cause and effect relationship between variables as opposed to the observational style of descriptive research (Anusree et al., 2014). Lastly, exploratory research differs from descriptive and casual research in that it is more qualitative in nature in that it focuses on the discovery of ideas and providing deeper insights (Anusree et al., 2014). As such, the research methodology adopted to address the research questions within Chapter 7 and 8 of this thesis is descriptive in nature.

According to Kothari (2004), the research methodology may be complemented by 2 research approaches. The first is a qualitative approach which is a subjective assessment of attitudes, opinions and behavior (Kothari, 2004). The second is a quantitative approach which focuses on the generation of data which may be subjected to quantitative analysis.

The quantitative approach, according to Kothari (2004), may be further classified as inferential (a sample of a population is studied, questioned or observed to identify characteristics that are inferred onto the overall population), experimental (specific variables may be manipulated to observe the effect on other variables) or simulation (creating an artificial environment to test conditions and generate data for further analysis).

As such, the research associated with Chapters 7 and 8 of this thesis is descriptive in nature and encompasses a quantitative inferential research approach executed through the use of an appropriate research instrument.

6.3 Research Instrumentation

The quantitative inferential research approach was executed through the use of a research survey as the preferred research instrument. This research survey is provided in Appendix D of this thesis and is referred to as the POPI research survey.

The POPI research survey consisted of an overview and contained 3 sections that comprised a total of 14 multiple choice questions which were carefully worded, unambiguous and objective. The first section of the POPI research survey, terms and conditions, had 1 question as listed below, which required all participants to electronically provide consent and to accept the terms and conditions of the POPI research survey before participating.

- Question 1: *Consent and Acceptance of Terms and Conditions*

The second section of the POPI research survey, qualifying questions, comprised the following 2 questions, which assessed the validity of the participant to undertake the POPI research survey:

- Question 2: *Does your organisation operate within South Africa?*
- Question 3: *Does your organisation within South Africa maintain electronic personal information and as a result is affected by the Protection of Personal Information (POPI) Act?*

The third section of the POPI research survey, main research questions, consisted of the following 11 questions aimed at addressing the research questions associated with Chapter 7 and 8 respectively. These 11 questions which were only made available to valid participants as a result of their institution operating in South Africa and maintaining electronic personal information, which resulted in them affected by the POPI Act (2013).

- Question 4: *How would you rate your overall level of understanding of the Protection of Personal Information (POPI) Act?*
- Question 5: *In which sector does your organisation operate?*
- Question 6: *Which industry sector best describes your organisation?*
- Question 7: *What is the size of your organisation?*
- Question 8: *How would you rate your organisation's overall compliance to the Protection of Personal Information (POPI) Act?*
- Question 9: *How would you rate your organisation's overall compliance to ensuring confidentiality (prevention of unauthorised disclosure) and integrity (prevention of unauthorised modification) of electronic personal information as required the Protection of Personal Information (POPI) Act?*
- Question 10: *What do you estimate is the financial value of electronic personal information maintained by your organisation?*
- Question 11: *What are the focus areas within your organisation presently to ensure confidentiality and integrity of electronic personal information as required by the Protection of Personal Information (POPI) Act (Multiple focus areas may be selected if applicable)?*
- Question 12: *What is the status of the following 20 safeguards within your organisation to ensure confidentiality and integrity of electronic personal information?*
- Question 13: *Are there any security safeguards your organisation has considered or implemented in addition to the 20 safeguards listed in question 12 to ensure confidentiality and integrity of electronic personal information?*
- Question 14: *How will a breach/compromise of electronic personal information impact your organisation (select the scenario below that will have the highest impact on your organisation)?*

Upon receiving approval from the Ethics Committee of the University of Pretoria as indicated in Appendix E of this thesis, the POPI research survey was launched online at https://www.surveymonkey.com/r/SAPOPI from 1 October 2015 to 15 December 2015.

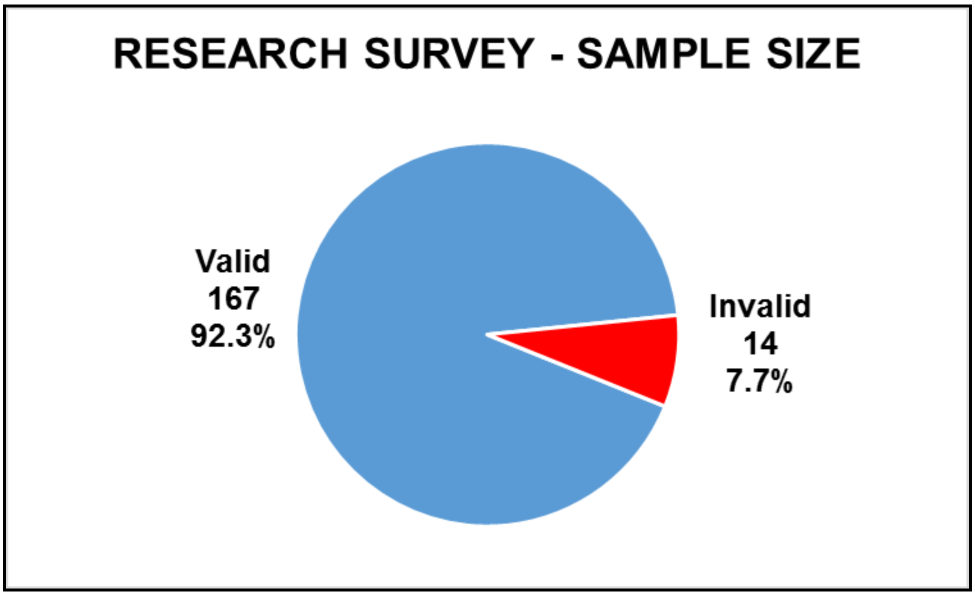
The POPI research survey targeted a specific research group and was completely anonymous as participants were not requested to provide any identifying information such as personal information (title, name, surname and email address) or the name of the institution which they represent.

6.4 Research Group

The research group specifically targeted by the POPI research survey were participants from South African institutions who store, process or transmit electronic personal information and as a result are impacted by the POPI Act (2013). A self-selection sampling technique was employed to attain the sample population inherent to the quantitative inferential research approach. This technique was suitable as it provided participants with the choice to either part take and complete the POPI research survey or not to part take in the research at all (Leard Dissertation, 2012).

Participants were informed of the POPI research survey via an email that included a link to the POPI research survey as well as through social media (Twitter and LinkedIn posts) and the South African Chapter of Information Systems Audit and Control Association (ISACA), who distributed the POPI research survey link to members of the South African chapter. Participants were also able to share the POPI research survey link with other participants within their network. As such, CIBECS assisted by distributing the POPI research survey link to participants who were targeted for the *2012 State of Business Data Protection in South Africa* survey (CIBECS, 2012).

From the date the POPI research survey was launched on 1 October 2015 to the date it closed on 15 December 2015, 181 participants completed the POPI research survey. However, only 167 research survey responses from participants were considered valid, as illustrated in Figure 6.1 on the next page. The criteria for a valid response to the POPI research survey was for a participant to be from an institution operating in South Africa and maintaining electronic personal information, which would mean that their institution is impacted by the POPI Act (2013).



Research survey validity	Response count	Response percentage
Valid	167	92.3%
Invalid	14	7.7%
Total	**181**	**100%**

Figure 6.1: POPI Research Survey - Sample Size

As a result, the sample size of the population associated with the POPI research survey was a total of 167 participants based on the valid research survey responses received. Therefore, the POPI research survey results subjected to data analysis is based on the 167 valid research survey responses from participants.

6.5 DATA ANALYSIS APPROACH

The data analysis approach to assess and summarise the POPI research survey results is represented through a combination of different types of graphs, charts and tables.

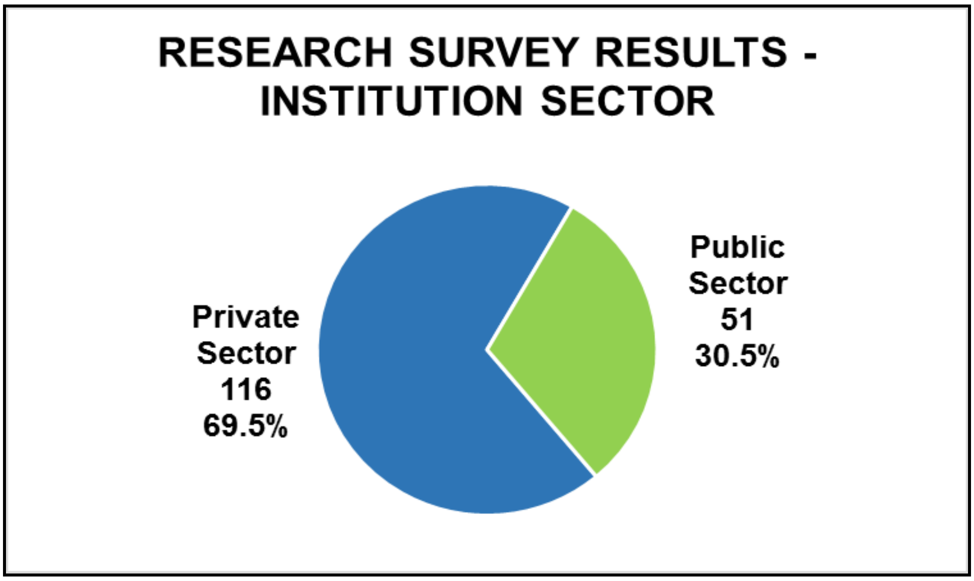
This data analysis approach is applied to the POPI research survey results to provide an overview of the demographics in terms of the 167 valid research survey responses from participants, in the next section of this chapter. Furthermore, the data analysis approach is applied to the POPI research survey results associated with Chapter 7 and 8 respectively, in order to ultimately address the research questions covered in these chapters.

6.6 POPI Research Survey Results - Demographics

The demographics associated with the 167 valid research survey responses received from participants were assessed in terms of a participant’s institution. This assessment was derived from a sector (public versus private), industry sector and institution size perspective, as the POPI Act is applicable to both public and private institutions in South Africa across all industry sectors, irrespective of their size.

6.6.1 Institution Sector

The sectors by differentiation of public or private sector that the 167 participants represented, is depicted in Figure 6.2 below.



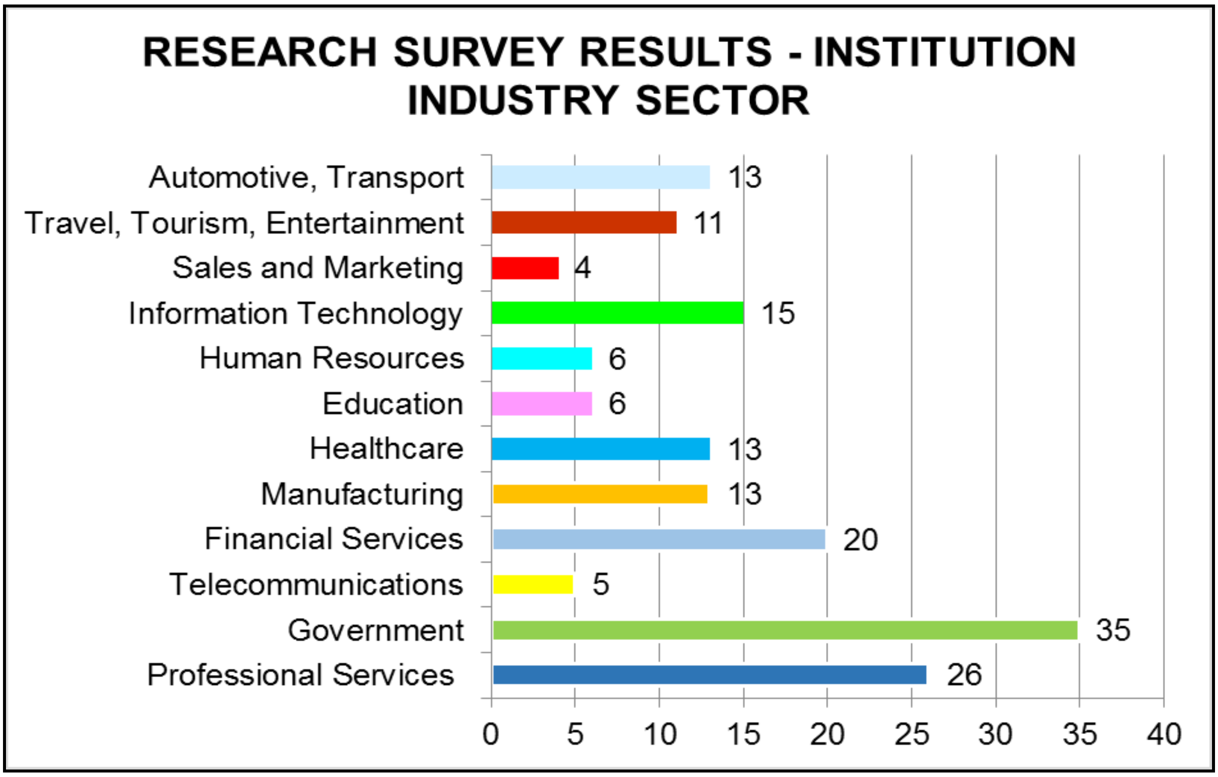
In which sector does your organisation operate?	Response Count	Response percentage
Private Sector	116	69.5%
Public Sector	51	30.5%
Total	**167**	**100%**

Figure 6.2: POPI Research Survey Results - Institution Sector

The majority of participants (69.5%) were from South African institutions in the private sector, while the remaining participants (30.5%) were from South African institutions in the public sector.

6.6.2 Institution Industry Sector

The industry sector in which the 167 participants' South African institutions operate in is depicted in Figure 6.3 below:



Which industry sector best describes your organisation?	Response count	Response percentage
Professional Services (Accounting, Legal, Engineering, Real Estate, Actuary, Consulting Services)	26	15.6%
Government	35	21.0%
Telecommunications	5	3.0%
Financial Services (Banking, Investments, Insurance)	20	12.0%
Manufacturing	13	7.8%
Healthcare	13	7.8%
Education	6	3.6%
Human Resources	6	3.6%
Information Technology	15	9.0%

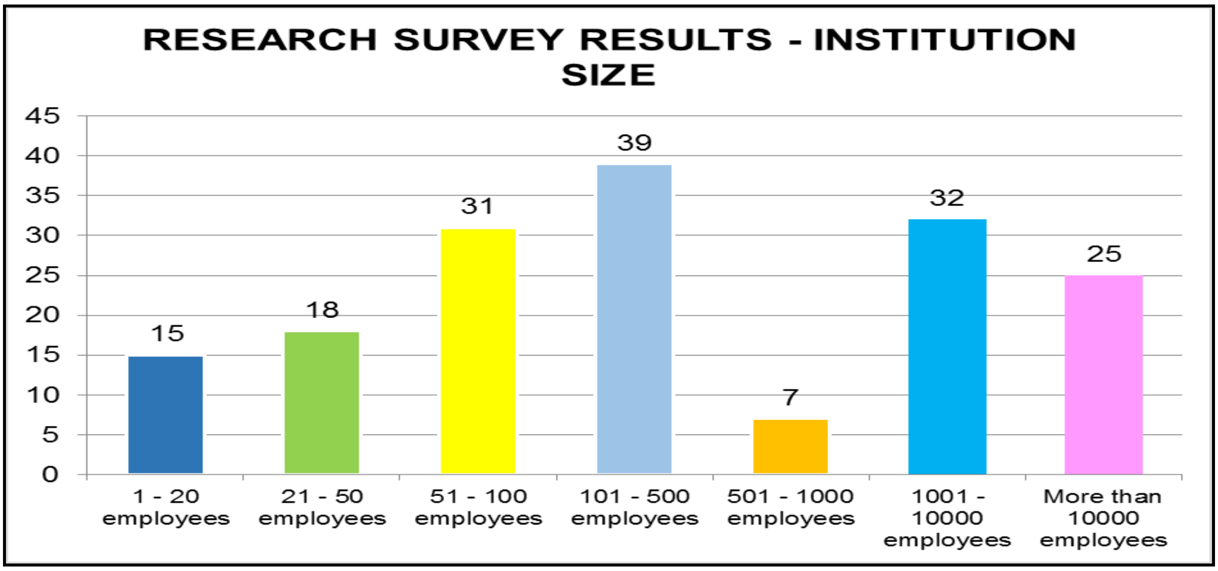
Which industry sector best describes your organisation?	Response count	Response percentage
Sales and Marketing	4	2.4%
Travel, Tourism, Entertainment	11	6.6%
Automotive, Transport	13	7.8%
Total	**167**	**100%**

Figure 6.3: POPI Research Survey Results - Institution Industry Sector

Participants were from South African institutions who operate within different industry sectors such as professional services (15.6%), government (21.0%), telecommunications (3.0%), financial services (12.0%), manufacturing (7.8%), healthcare (7.8%), education (3.6%), human resources (3.6%), information technology (9.0%), sales and marketing (2.4%), travel, tourism, entertainment (6.6%) and automotive, transport (7,8%).

6.6.3 Institution Size

The size of the South African institutions which the 167 participants operate in (as determined by the number of employees at their respective institutions) is depicted in Figure 6.4 below:



What is the size of your organisation?	Response count	Response percentage
1 - 20 employees	15	9.0%
21 - 50 employees	18	10.8%

What is the size of your organisation?	Response count	Response percentage
51 - 100 employees	31	18.6%
101 - 500 employees	39	23.4%
501 - 1000 employees	7	4.2%
1001 - 10000 employees	32	19.2%
More than 10000 employees	25	15.0%
Total	**167**	**100%**

Figure 6.4: POPI Research Survey Results - Institution Size

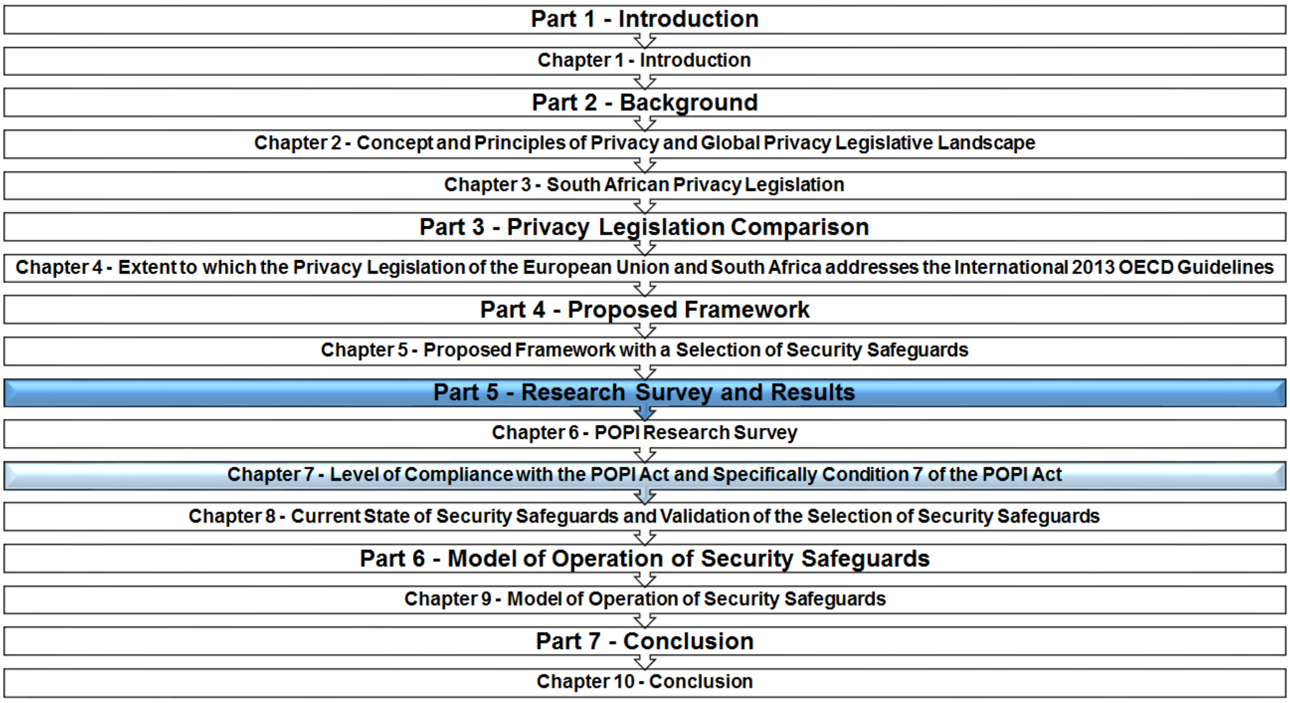
The majority of participants (23.4%) were from South African institutions which had an employee count of between 101 and 500 employees. This was followed by 19.2% of participants who were from South African institutions who had an employee count of between 1001 and 10000 employees. There were also 15.0% of participants who had an employee count of more than 10000 employees.

6.7 CONCLUSION

This chapter in terms of Part 5 (Research Survey and Results) of this thesis provided an overview of the POPI research survey which included the research design, research instrumentation, research group and the data analysis approach. Furthermore, the demographics associated with the POPI research survey results obtained was assessed in terms of a participant’s institution. This assessment was from a sector (public versus private), industry sector and institution size perspective as the POPI Act is applicable to both public and private institutions in South Africa across all industry sectors, irrespective of their size.

The research questions associated with Chapter 7 and 8 respectively, which follow this chapter, are addressed through an analysis of the 167 valid research survey responses from participants, who completed the POPI research survey.

CHAPTER 7 - LEVEL OF COMPLIANCE WITH THE POPI ACT AND SPECIFICALLY CONDITION 7 OF THE POPI ACT



Part 1 - Introduction

Chapter 1 - Introduction

Part 2 - Background

Chapter 2 - Concept and Principles of Privacy and Global Privacy Legislative Landscape

Chapter 3 - South African Privacy Legislation

Part 3 - Privacy Legislation Comparison

Chapter 4 - Extent to which the Privacy Legislation of the European Union and South Africa addresses the International 2013 OECD Guidelines

Part 4 - Proposed Framework

Chapter 5 - Proposed Framework with a Selection of Security Safeguards

Part 5 - Research Survey and Results

Chapter 6 - POPI Research Survey

Chapter 7 - Level of Compliance with the POPI Act and Specifically Condition 7 of the POPI Act

Chapter 8 - Current State of Security Safeguards and Validation of the Selection of Security Safeguards

Part 6 - Model of Operation of Security Safeguards

Chapter 9 - Model of Operation of Security Safeguards

Part 7 - Conclusion

Chapter 10 - Conclusion

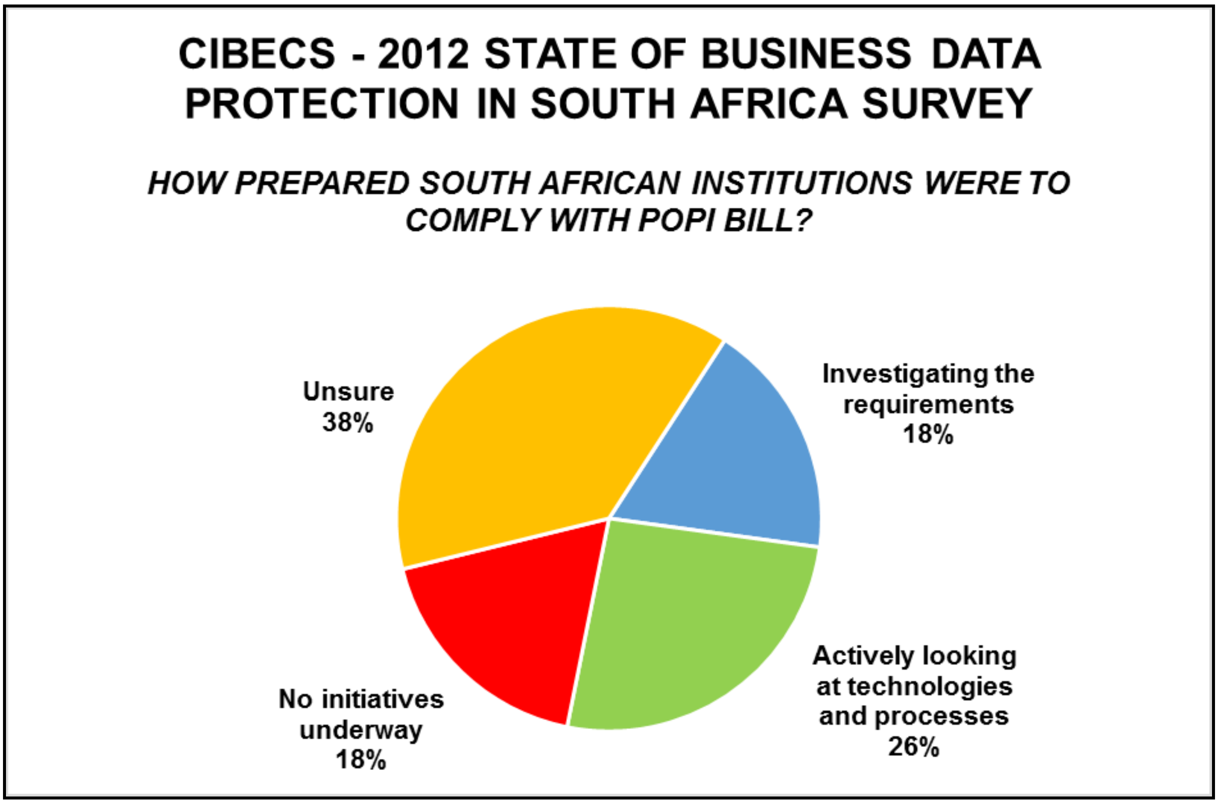
7.1 INTRODUCTION

Chapter 6 provided an overview of the POPI research survey which included the research design, research instrumentation, research group and the data analysis approach. Furthermore, Chapter 6 assessed the demographics associated with the POPI research survey results in terms of the participant's institution. This chapter, utilising the POPI research survey results from 167 participants, addresses research question 3 - *What is the current level of compliance by South African institutions to the POPI Act (2013) and specifically Condition 7 of the POPI Act (2013)?*

This is achieved by providing an overview of the *State of Business Data Protection in South Africa* survey (CIBECS, 2012) conducted in 2012 and analysing the POPI research survey results. Firstly, the analysis of the POPI research survey results provides the overall level of understanding of the Protection of Personal Information (POPI) Act (Act 4 of 2013) by the 167 participants who took part in the POPI research survey. Secondly, the analysis addresses the aforementioned research question by providing the current level of compliance with the POPI Act (2013) as well as with Condition 7 of the Act. Lastly, the POPI research survey results provide the financial value associated with electronic personal information as well as the potential impact of a data breach of electronic personal information. In addition, a critical evaluation in terms of key findings and recommendations based on the analysis of the POPI research survey results is provided.

7.2 2012 STATE OF BUSINESS DATA PROTECTION IN SOUTH AFRICA

In 2012, CIBECS as part of their *State of Business Data Protection in South Africa* survey (CIBECS, 2012) assessed, among other aspects, how prepared South African institutions were to comply with the then forthcoming protection of personal information legislation. As per Figure 7.1 on the next page, the results of the survey revealed that 38% of participants were unsure of the how prepared their institutions were to comply with the then forthcoming protection of personal information legislation (CIBECS, 2012). Furthermore, 18% of participants stated that no initiatives were underway to ensure compliance (CIBECS, 2012). However, 26% of participants were actively looking at technologies and processes to ensure compliance, while 18% of participants were investigating the requirements but not actively pursuing compliance with the then forthcoming protection of personal information legislation (CIBECS, 2012).



CIBECS category – 2012	Response percentage
Investigating the requirements but not actively pursuing compliance	18%
Actively looking at technologies and processes to ensure compliance	26%
No initiatives were underway to ensure compliance with the forthcoming protection of personal information legislation	18%
Unsure of the how prepared their institutions were to comply with the forthcoming protection of personal information legislation	38%
Total	**100%**

Figure 7.1: 2012 State of Business Data Protection in South Africa Survey

Source: Adapted from CIBECS (2017)

7.3 POPI Research Survey Results - Analysis

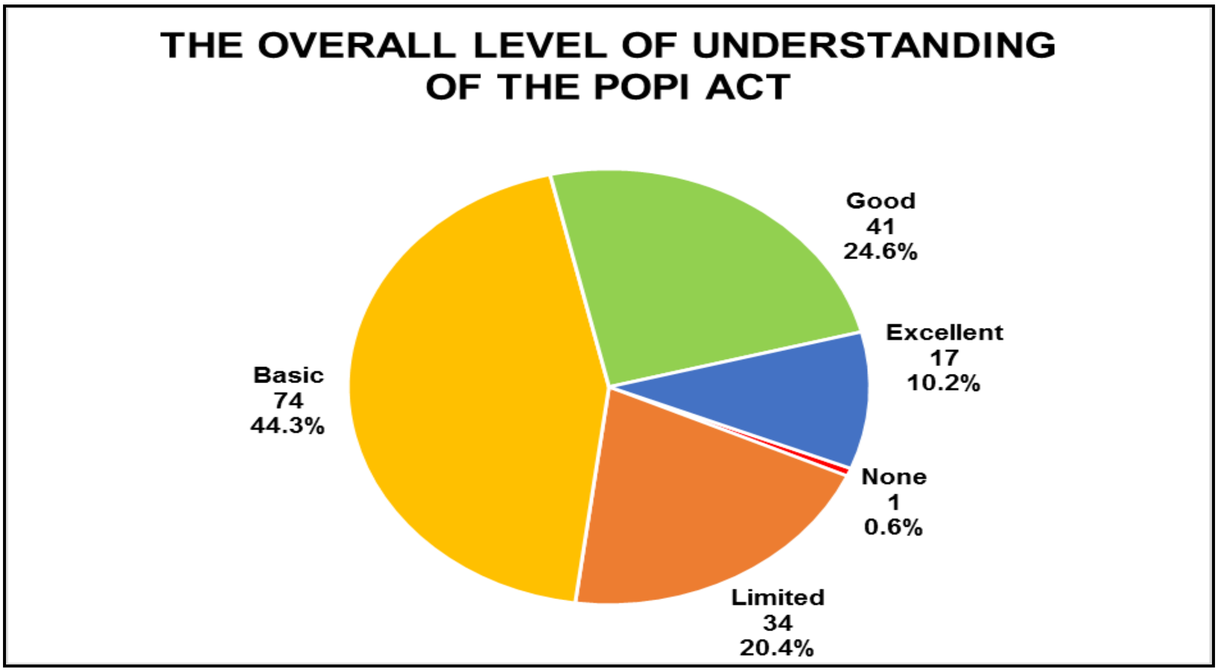
Since the *State of Business Data Protection in South Africa* survey (CIBECS, 2012), the POPI Bill progressed to an Act and thus presented an opportunity to analyse the progress made by South African institutions in terms of the following aspects listed below:

- The overall level of understanding of the POPI Act (2013).
- The current level of compliance with the POPI Act (2013).
- The current level of compliance with Condition 7 of the POPI Act (2013).
- The financial value associated with electronic personal information.
- The potential impact of a data breach of electronic personal information.

As such, the POPI research survey results associated with 167 participants who completed the POPI research survey is analysed from subsection 7.3.1 to 7.3.5 to address the aforementioned aspects.

7.3.1 The Overall Level of Understanding of the POPI Act

The overall level of understanding of the POPI Act (2013) by the 167 participants from South African institutions is depicted in Figure 7.2 below:



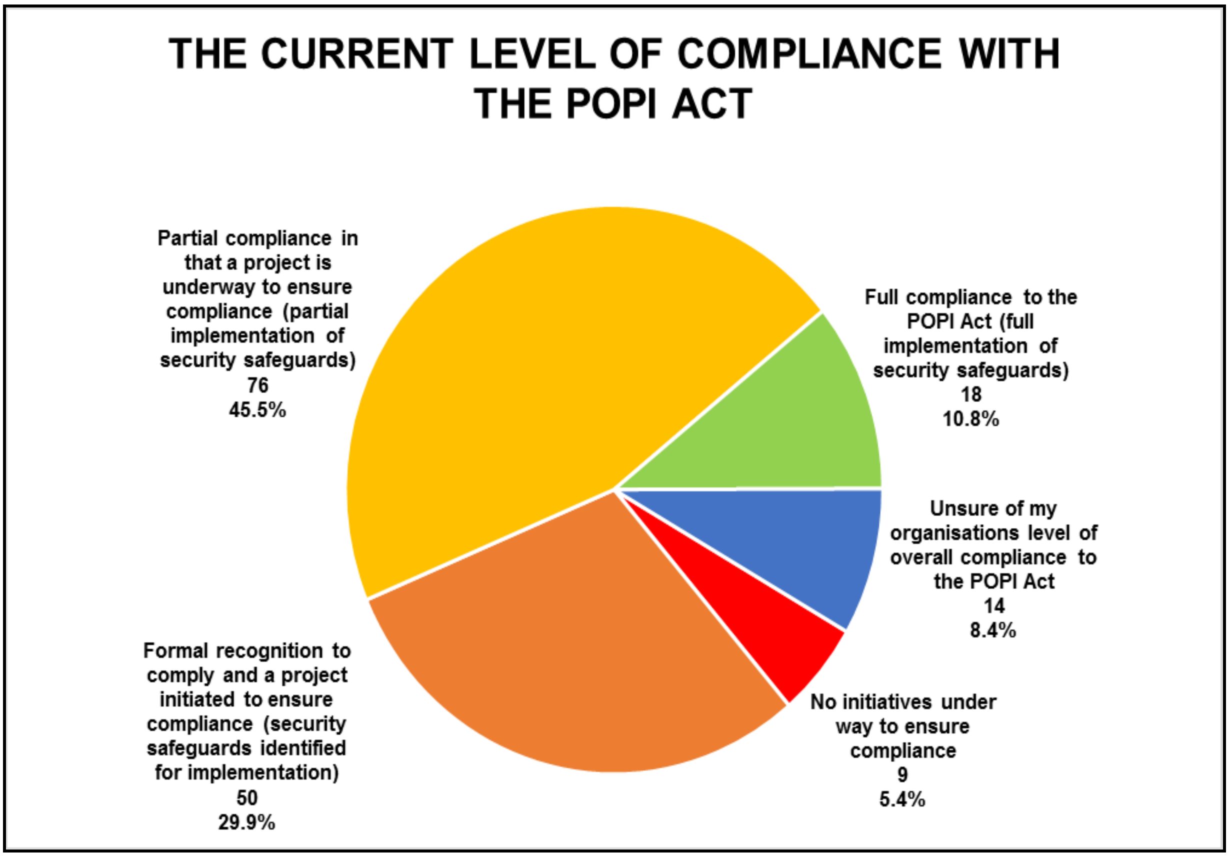
How would you rate your overall level of understanding of the Protection of Personal Information (POPI) Act?	Response count	Response percentage
None	1	0.6%
Limited	34	20.4%
Basic	74	44.3%
Good	41	24.6%
Excellent	17	10.2%
Total	**167**	**100%**

Figure 7.2: The Overall Level of Understanding of the POPI Act

The majority of participants (44.3%) had a basic overall level of understanding of the POPI Act (2013). This was followed by 24.6% of participants who had a good overall level of understanding as opposed to 10.2% of participants who had an excellent overall level understanding of the POPI Act (2013). A limited overall understanding of the POPI Act (2013) was applicable to 20.4% of participants with only 1 participant (0.6%) possessing no overall level understanding of the POPI Act (2013).

7.3.2 THE CURRENT LEVEL OF COMPLIANCE WITH THE POPI ACT

The assessment of the current level of compliance with the POPI Act (2013) by South African institutions as provided by the 167 participants of the POPI research survey, provided in Figure 7.3 on the next page, addresses the research question associated with this chapter as outlined in the Introduction above.



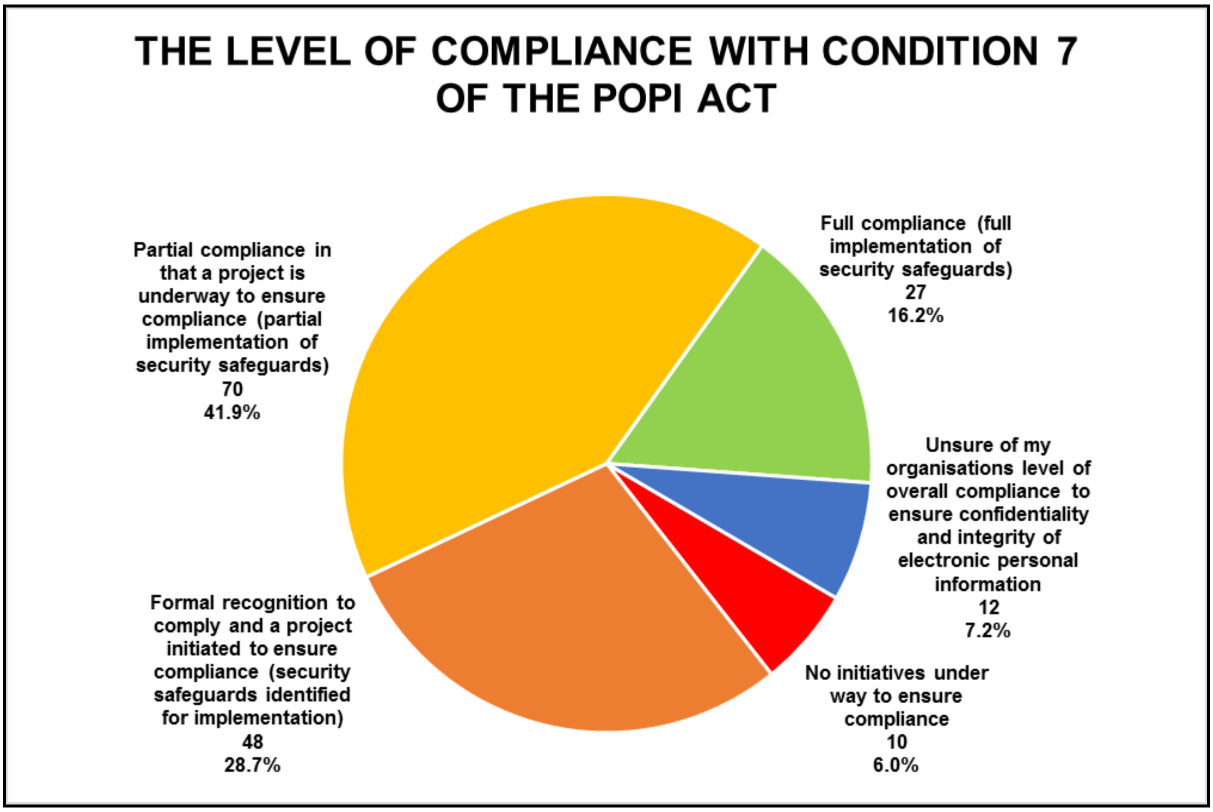
How would you rate your institution's overall compliance to the POPI Act?	Response count	Response percentage
No initiatives under way to ensure compliance	9	5.4%
Formal recognition to comply and a project initiated to ensure compliance (security safeguards identified for implementation)	50	29.9%
Partial compliance in that a project is underway to ensure compliance (partial implementation of security safeguards)	76	45.5%
Full compliance to the POPI Act (full implementation of security safeguards)	18	10.8%
Unsure of my institution's level of overall compliance to the POPI Act	14	8.4%
Total	**167**	**100%**

Figure 7.3: The Current Level of Compliance with the POPI Act

As per Figure 7.3 above, the majority of participants (45.5%) stated that their respective institutions was partially complying to the POPI Act (2013), in other words, that a project is underway to ensure compliance and security safeguards are partially implemented. Formal recognition to comply with the POPI Act (2013), and as such a project was initiated to ensure compliance with the legislation, was applicable to 29.9% of the participants. However, 8.4% of participants were unsure of their institutions' level of overall compliance with the POPI Act (2013). Furthermore, 5.4% of participants stated that no initiatives were underway in their institutions to ensure compliance with the POPI Act (2013). However, 10.8% of participants stated that their institutions fully comply with the POPI Act (2013), implying that security safeguards are fully implemented.

7.3.3 The Current Level of Compliance with Condition 7 of the POPI Act

Taking into account the level of overall compliance with the POPI Act (2013) the second aspect of the research question associated with this chapter as outlined in the Introduction section above is provided in Figure 7.4 below. This assessment explored the level of compliance with Condition 7 of the POPI Act (2013) by South African institutions as provided by the 167 participants of the POPI research survey, specifically relating to the confidentiality and integrity of electronic personal information.



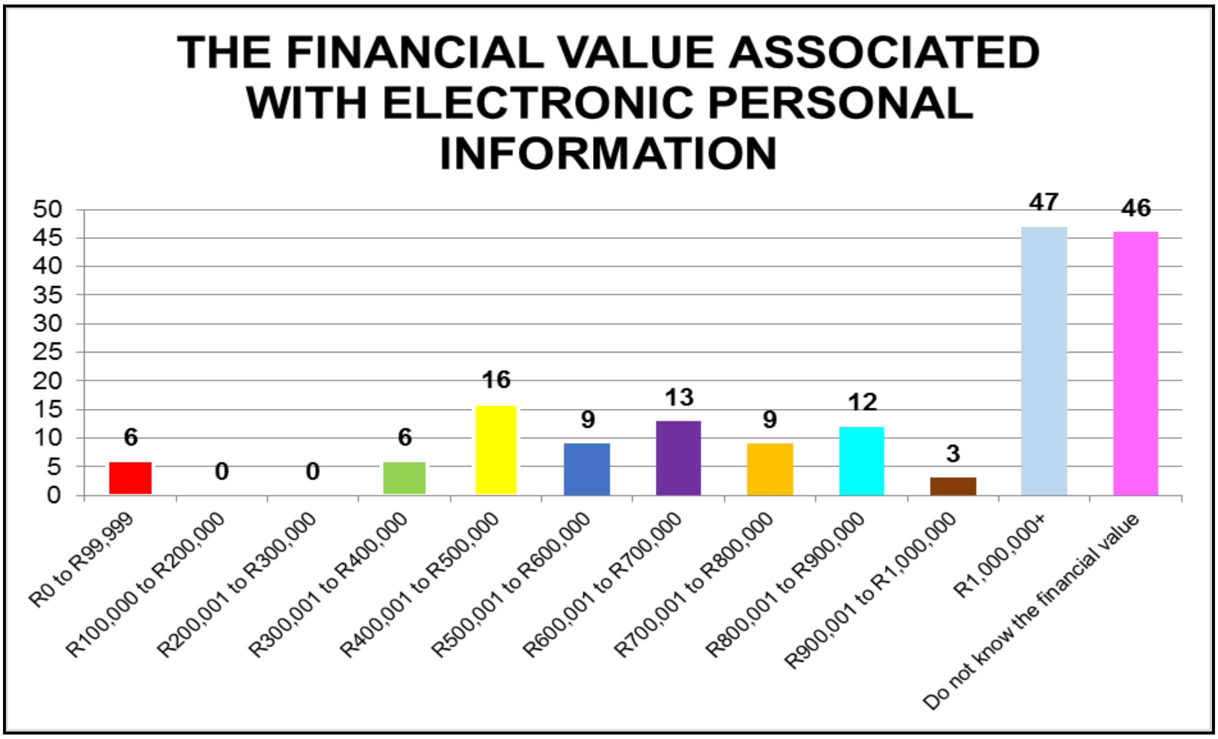
How would you rate your institutions overall compliance to ensuring confidentiality (prevention of unauthorised disclosure) and integrity (prevention of unauthorised modification) of electronic personal information as required by the POPI Act?	**Response count**	**Response percentage**
No initiatives under way to ensure compliance	10	6.0%
Formal recognition to comply and a project initiated to ensure compliance (security safeguards identified for implementation)	48	28.7%
Partial compliance in that a project is underway to ensure compliance (partial implementation of security safeguards)	70	41.9%
Full compliance (full implementation of security safeguards)	27	16.2%
Unsure of my institutions level of overall compliance to ensure confidentiality and integrity of electronic personal information	12	7.2%
Total	**167**	**100%**

Figure 7.4: The Level of Compliance with Condition 7 of the POPI Act

The majority of participants (41.9%) stated that their respective institution was partially complying in terms of ensuring confidentiality and integrity of electronic personal information as required by Condition 7 of the POPI Act (2013), in that a project is underway to ensure compliance. There is formal recognition to comply with ensuring the confidentiality and integrity of electronic personal information as required by Condition 7 of the POPI Act (2013) and as such, a project was initiated to ensure compliance, which was applicable to 28.7% of the participants. However, 7.2% of participants were unsure of their institutions' level of compliance to ensure the confidentiality and integrity of electronic personal information as required by Condition 7 of the POPI Act (2013). Furthermore, 6.0% of participants stated that no initiatives were underway in their institutions to ensure the confidentiality and integrity of electronic personal information as required by Condition 7 of the POPI Act (2013). However, 16.2% of participants stated that their institutions fully comply with ensuring the confidentiality and integrity of electronic personal information as required by Condition 7 of the POPI Act (2013).

7.3.4 The Financial Value Associated with Electronic Personal Information

Participants also provided a view on the financial value associated with the electronic personal information maintained by their respective institutions, as illustrated in Figure 7.5 below.



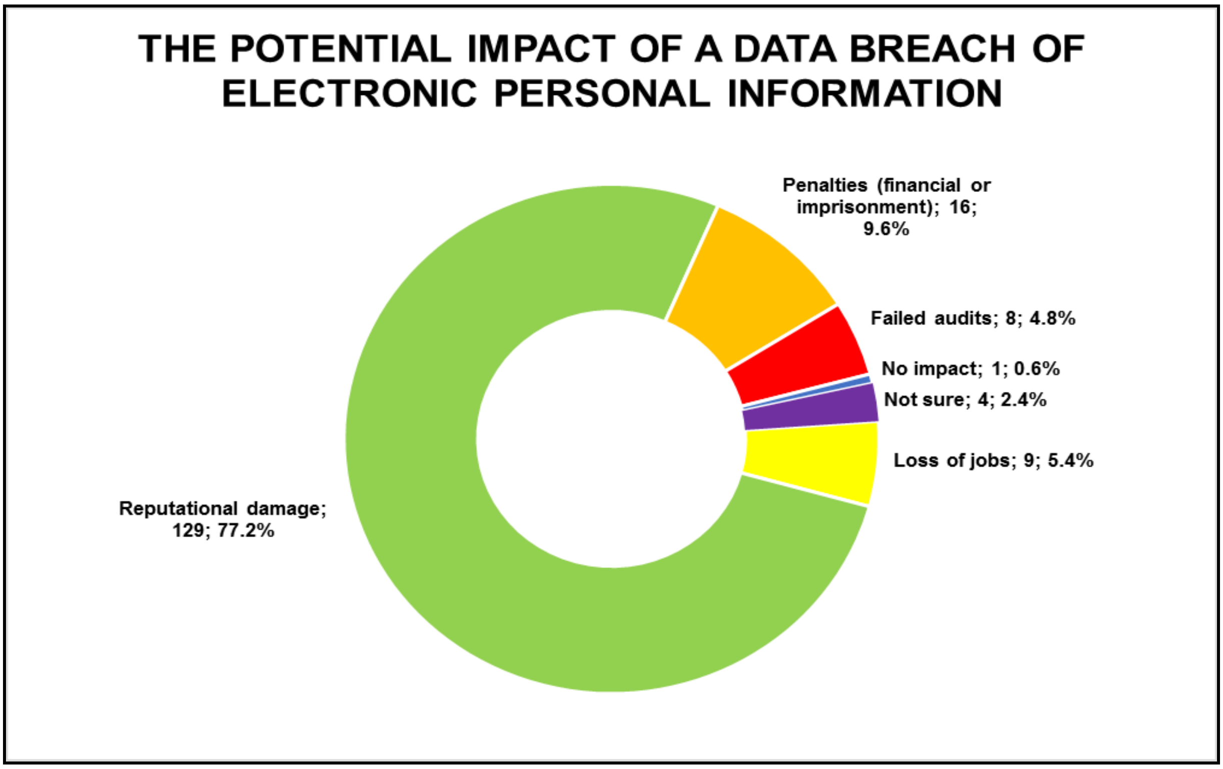
What do you estimate is the financial value of electronic personal information maintained by your institution?	Response count	Response percentage
R0 to R99,999	6	3.6%
R100,000 to R200,000	0	0.0%
R200,001 to R300,000	0	0.0%
R300,001 to R400,000	6	3.6%
R400,001 to R500,000	16	9.6%
R500,001 to R600,000	9	5.4%
R600,001 to R700,000	13	7.8%
R700,001 to R800,000	9	5.4%
R800,001 to R900,000	12	7.2%
R900,001 to R1,000,000	3	1.8%
R1,000,000+	47	28.1%
Do not know the financial value	46	27.5%
Total	**167**	**100%**

Figure 7.5: The Financial Value Associated with Electronic Personal Information

In terms of the financial value associated with electronic personal information, the majority of participants (28.1%) assigned a value in excess of R1 million. A number of participants (27.5%) did not know the financial value associated with electronic personal information maintained by their respective institutions. However, the remaining 44.4% of participants could allocate a financial value ranging from R0 to R1 million.

7.3.5 The Potential Impact of a Data Breach of Electronic Personal Information

As illustrated in Figure 7.6 below, participants provided a view of the potential impact a data breach of electronic personal information may have on their respective institutions.



How will a breach/compromise of electronic personal information impact your institution (select the scenario below that will have the highest impact on your institution)?	Response count	Response percentage
Loss of jobs	9	5.4%
Reputational damage	129	77.2%
Penalties (financial or imprisonment)	16	9.6%
Failed audits	8	4.8%
No impact	1	0.6%

How will a breach/compromise of electronic personal information impact your institution (select the scenario below that will have the highest impact on your institution)?	Response count	Response percentage
Not sure	4	2.4%
Total	**167**	**100%**

Figure 7.6: The Potential Impact of a Data Breach of Electronic Personal Information

The highest impact of a data breach of electronic personal information would be reputational damage to the institution, according to 77.2% of participants. This was followed by penalties (financial or imprisonment) which account for 9.6% of participants, loss of jobs which account for 5.4% of participants and failed audits which account for 4.8% of participants. However, 2.4% of participants were unsure of the impact of a data breach of electronic personal information and 1 participant (0.6%) stated that a data breach of electronic personal information would have no impact.

7.4 Critical Evaluation - Key Findings and Recommendations

The analysis of the POPI research survey results forms the basis of the critical evaluation in terms of key findings and recommendations as it relates to the following aspects:

- The overall level of understanding of the POPI Act (2013).
- The current level of compliance with the POPI Act (comparison between the 2012 CIBECS survey and POPI research survey conducted as part of this thesis in 2015).
- Comparing the overall compliance with the POPI Act (2013) to the overall compliance with Condition 7 of the Act.
- The financial value associated with electronic personal information.
- The potential impact of a data breach of electronic personal information.

The key findings and recommendations associated with the aforementioned aspects follow from subsection 7.4.1 to 7.4.5 below.

7.4.1 THE OVERALL LEVEL OF UNDERSTANDING OF THE POPI ACT

The overall level of understanding of the POPI Act (2013) at the time of the POPI research survey being conducted was at a basic level (44.3% of the participants). As a result, given that the commencement date of the POPI Act (2013) has not been announced and as such the POPI Act (2013) is not yet enforceable, there is a window of opportunity that exists to increase the level of understanding from basic to good or excellent via formal training and awareness sessions in order to successfully drive initiatives to ensure compliance with the POPI Act (2013) and to address areas of non-compliance.

7.4.2 THE CURRENT LEVEL OF COMPLIANCE WITH THE POPI ACT (COMPARISON BETWEEN 2012 AND 2015)

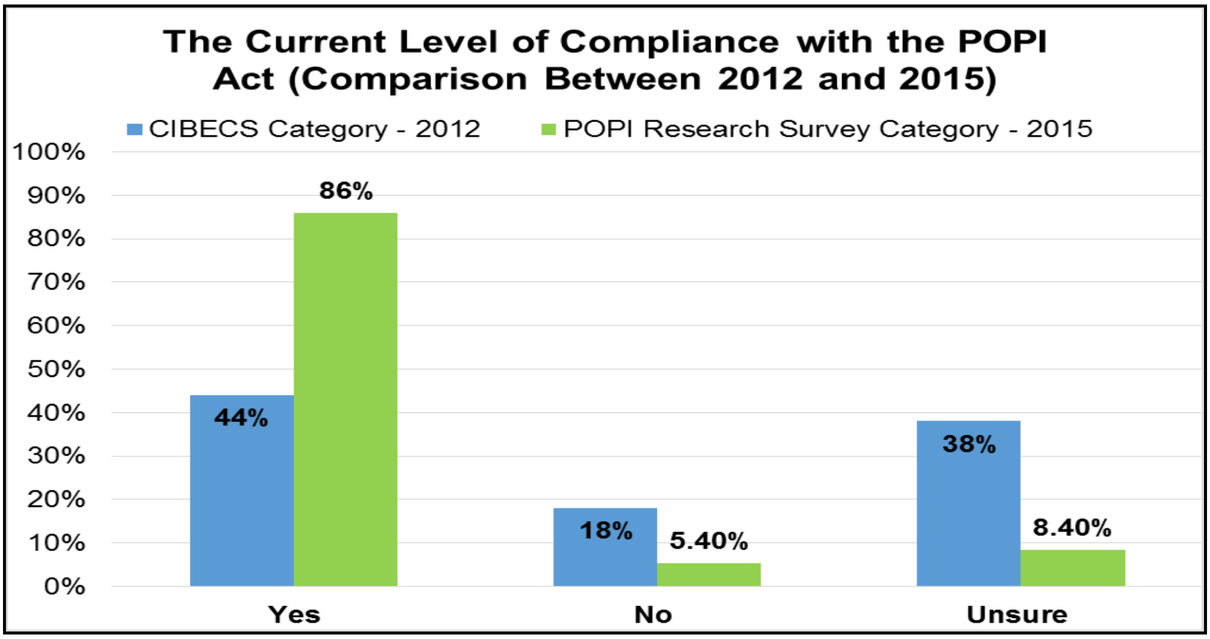
In order to compare the level of compliance with the POPI Act (2013) by South African institutions in 2015 to the level of compliance shown in 2012 as per the *State of Business Data Protection in South Africa* survey conducted by CIBECS (2012), the grouping as illustrated in Table 7.1 below was performed to ascertain the common categories for comparison. The rationale for ascertaining common categories for comparison is that in 2012 the Protection of Personal Information legislation was still at the stage of a Bill and once it was enacted as the POPI Act (2013), formal initiatives to comply had commenced. In both research surveys, participants stated “No” initiatives were underway to comply or they were “Unsure” of the level of compliance with the protection of personal information legislation, resulting in a direct link in the formulation of the two of the three common categories for comparison. However, the third common category termed “Yes” was formulated by grouping together all activities towards achieving compliance from investigation to formal recognition and partial compliance as well as full compliance with the POPI Act (2013).

Table 7.1: Formulation of Common Categories for Comparison

CIBECS category - 2012	POPI research survey category - 2015	Common category formulated for comparison
Investigating the requirements but not	Formal recognition to comply and a project	Yes

CIBECS category - 2012	POPI research survey category - 2015	Common category formulated for comparison
actively pursuing compliance - 18% Actively looking at technologies and processes to ensure compliance - 26%	initiated to ensure compliance (security safeguards identified for implementation) - 29.9% Partial compliance in that a project is underway to ensure compliance (partial implementation of security safeguards) - 45.5% Full compliance to the POPI Act (full implementation of security safeguards) - 10.8%	
No initiatives were underway to ensure compliance with the forthcoming protection of personal information legislation - 18%	No initiatives under way to ensure compliance - 5.4%	No
Unsure of the how prepared their institutions were to comply with the forthcoming protection of personal information legislation - 38%	Unsure of my institutions level of overall compliance to the POPI Act - 8.4%	Unsure

The comparison between the current level of compliance with the POPI Act (2013) by South African institutions in 2015 to the previous level of compliance as per the *2012 State of Business Data Protection in South Africa* survey conducted by CIBECS (2012) is provided in Figure 7.7 below, utilising the common categories formulated in Table 7.1 on the previous page.



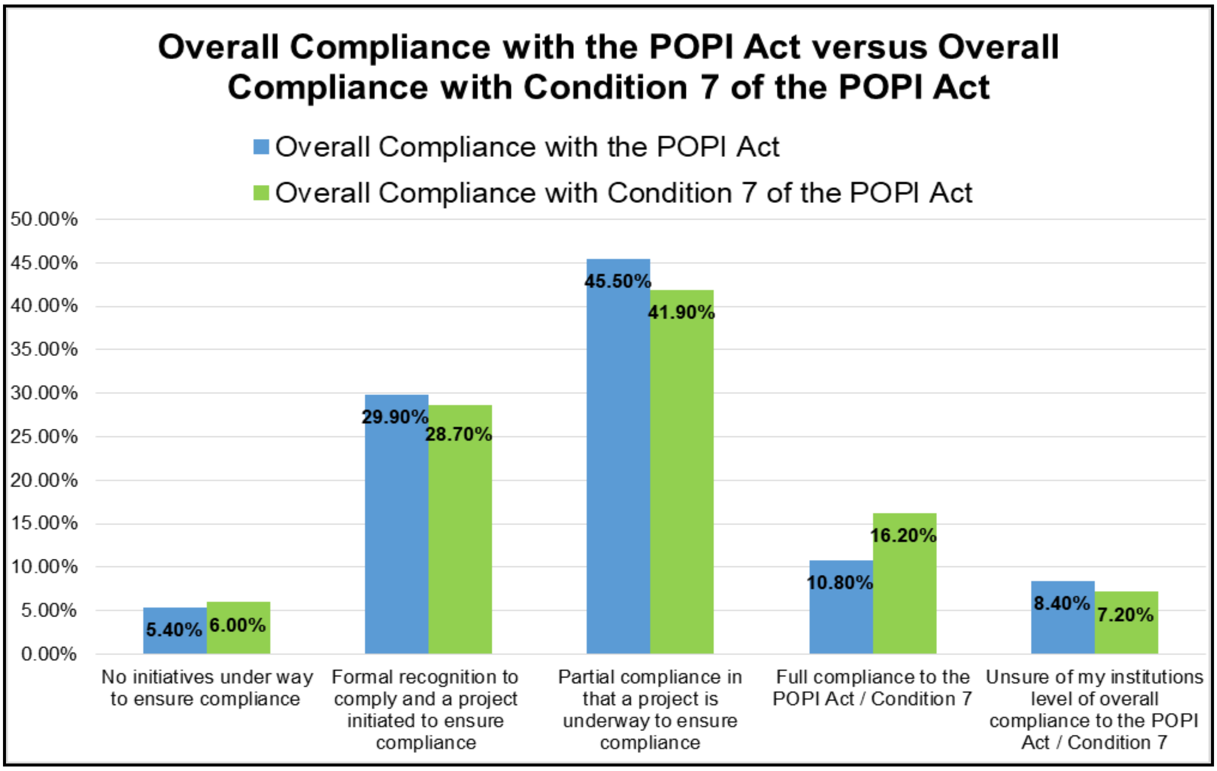
Common category formulated for comparison	CIBECS category - 2012	POPI research survey category - 2015
Yes	44%	86%
No	18%	5.4%
Unsure	38%	8.4%

Figure 7.7: The Current Level of Compliance with the POPI Act (Comparison between 2012 and 2015)

The POPI research survey conducted in 2015 illustrated a significant increase towards achieving compliance with the POPI Act (2013) from 44% to 86% of the participants. This can be attributed to the fact that the POPI Act (2013) was signed into law on 26 November 2013. Furthermore, in 2015 processes commenced to setup the Office of the Information Regulator (Parliament of the Republic of South Africa, 2015), who would be responsible for enforcing the POPI Act (2013). On 26 October 2016, the President of South Africa announced the appointment of Advocate Pansy Tlakula as the chair, Advocate Cordelia Stroom and Mr Johannes Weapond as full-time members, and Professor Tana Pistorius and Mr Sizwe Snail as part-time members of the Office of the Information Regulator, with effect from 1 December 2016 (Michalsons, 2016). As a result, the commencement date of the POPI Act (2013) may be looming on the horizon leaving South African public and private institutions with one year to comply. Therefore, it is critical that South African institutions continue the momentum to ultimately achieve and maintain full compliance with the POPI Act (2013) as the short timeframe to comply may not be sufficient if compliance initiatives are embarked upon only once the commencement date is announced. However, it is encouraging to note the significant decrease in participants who stated “No” initiatives (from 18% to 5.4% of participants) were underway to ensure compliance with the POPI Act (2013) or they were “Unsure” of the level of compliance (from 38% to 8.4%) to the POPI Act (2013) by their respective institutions.

7.4.3 Overall Compliance with the POPI Act versus Overall Compliance with Condition 7 of the POPI Act

An analysis of the overall level of compliance with the POPI Act (2013) compared to the overall level of compliance to ensure confidentiality and integrity of electronic personal information as required by Condition 7 of the POPI Act (2013) is provided in Figure 7.8 on the next page. This analysis is critical to ensure that compliance with the POPI Act (2013) does not neglect electronic personal information.



Level of compliance category	Overall compliance with the POPI Act	Overall compliance with Condition 7 of the POPI Act	Variance
No initiatives under way to ensure compliance	5.4%	6.0%	+0.6%
Formal recognition to comply and a project initiated to ensure compliance (security safeguards identified for implementation)	29.9%	28.7%	-1.2%
Partial compliance in that a project is underway to ensure compliance (partial implementation of security safeguards)	45.5%	41.9%	-3.6%
Full compliance to the POPI Act / Condition 7 (full implementation of security safeguards)	10.8%	16.2%	+5.4%
Unsure of my institutions level of overall compliance to the POPI Act / Condition 7	8.4%	7.2%	-1.2%

Figure 7.8: Overall Compliance with the POPI Act versus Overall Compliance with Condition 7 of the POPI Act

In the data table associated with Figure 7.8 on the previous page, a positive variance reflects the overall level of compliance with Condition 7 of the POPI Act (2013), in terms of ensuring confidentiality and integrity of electronic personal information for a particular compliance category, to be higher than the overall level of compliance with the entire POPI Act (2013). In comparison, a negative variance reflects the overall level of compliance with Condition 7 of the Act, in terms of ensuring confidentiality and integrity of electronic personal information for a particular compliance category to be lower than the overall level of compliance with the entire POPI Act (2013). As such, the positive and negative variances for 4 of the 5 categories did not exceed 5%, as per the data table associated with Figure 7.8 on the previous page. This illustrates a degree of alignment between the overall initiative to achieve compliance with the POPI Act (2013) and at the same time, to address the requirements of Condition 7 of the Act to ensure the confidentiality and integrity of electronic personal information. For example, 8.4% of participants were unsure of the overall level of compliance with the POPI Act (2013) and 7.2% of participants were unsure of the level of compliance in ensuring confidentiality and integrity of electronic personal information. One compliance category exceeded 5%, as per the data table associated with Figure 7.8 on the previous page, and it related to full compliance. This demonstrates that there is a greater level of compliance to ensure confidentiality and integrity of electronic personal information as opposed to the overall level of compliance with the entire POPI Act (2013). This does not pose a major threat as the overall level of compliance with the POPI Act (2013) takes into account several other requirements, for example, non-electronic personal information. However, it is critical to ensure that the POPI compliance initiative is adequate and comprehensive to address all requirements to ultimately achieve compliance with the POPI Act (2013), without neglecting any requirement.

7.4.4 The Financial Value Associated with Electronic Personal Information

The majority of participants (72.5%) associated a financial value to the electronic personal information maintained by their institutions. 28.1% of participants assigned a value in excess of 1 million rand while 44.4% of participants associated a financial value ranging from 0 to 1 million rand. However, the remaining 27.5% of participants could not associate a financial value to the electronic personal information maintained by their respective institutions. This may pose a challenge in terms of justifying the costs associated with the safeguards required to ensure confidentiality and integrity of electronic personal information. For example, if the financial value of electronic personal information is R900 000, the safeguards to ensure confidentiality and integrity of electronic personal information should generally not exceed R900 000. In addition, understanding the financial value of electronic personal information together with the costs of safeguards to ensure confidentiality and integrity of electronic personal information will strengthen the business case relating to the POPI compliance initiative. Furthermore, in the event of a data breach of electronic personal information a financial value may be associated with the loss of electronic personal information. Therefore, it is critical to ensure that a financial value is associated with electronic personal information within the institution and the most opportune time to associate a financial value would be when the electronic personal information is identified within the institution and the need for storing, processing or transmitting the electronic personal information is understood.

7.4.5 The Impact of a Data Breach of Electronic Personal Information

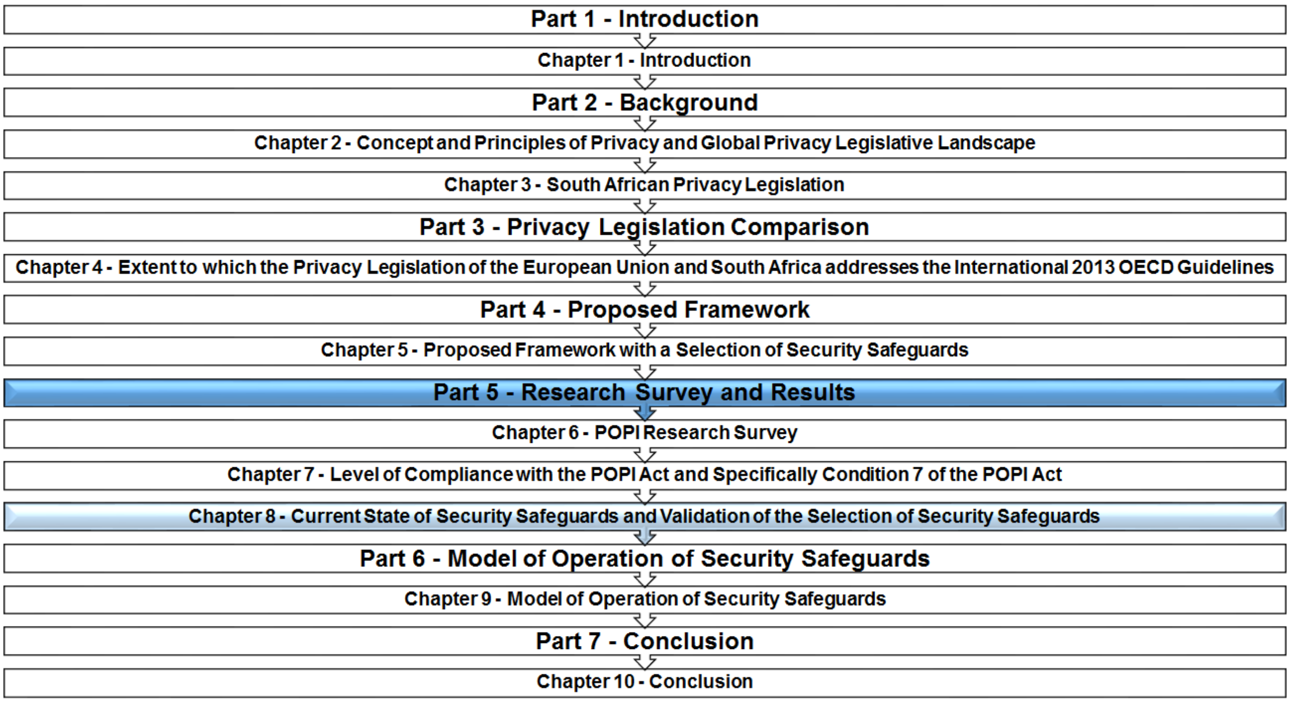
Reputational damage to an institution was rated to have the highest impact in the event of a data breach of electronic personal information by 77.2% of participants. This was followed by penalties (financial or imprisonment) which account for 9.6% of participants. Reputational damage will remain a high impact area in the event of a data breach of electronic personal information. However, once the POPI Act (2013) is enforced and if not complied with, members of the South African public and private institutions may be fined up to 10 million rand, face imprisonment not exceeding 10 years or receive a combination of a fine and imprisonment. This may lead to an increase in the number of participants who associate the impact of a data breach with penalties (financial or imprisonment). Therefore, it will be in the best interests of South African institutions to ensure compliance with the POPI Act (2013) given the aforementioned implications associated with a data breach.

7.5 CONCLUSION

This chapter, in terms of Part 5 (Research Survey and Results) of this thesis, provided an overview of the *State of Business Data Protection in South Africa* survey (CIBECS, 2012) conducted in 2012 and analysed the POPI research survey results in order to address the research question associated with this chapter. Firstly, the analysis of the POPI research survey results provided the overall level of understanding of the POPI Act (2013) by the 167 participants who took part in the POPI research survey. Secondly, the analysis addressed the research question associated with this chapter by providing the current level of compliance with the POPI Act (2013) as well as with Condition 7 of the Act. Lastly, the POPI research survey results provided the financial value associated with electronic personal information as well as the potential impact of a data breach of electronic personal information. In addition, a critical evaluation in terms of key findings and recommendations based on the analysis of the POPI research survey results was provided.

Part 5 (Research Survey and Results) of this thesis also consists of the next chapter which provides the current state of security safeguards within South African institutions to achieve compliance with Condition 7 of the POPI Act (2013), specifically in relation to electronic personal information. In addition, the validity of the selection of security safeguards proposed as part of the proposed POPI Condition 7 framework within Chapter 5 is also assessed.

CHAPTER 8 - CURRENT STATE OF SECURITY SAFEGUARDS AND VALIDATION OF THE SELECTION OF SECURITY SAFEGUARDS



Part 1 - Introduction

Chapter 1 - Introduction

Part 2 - Background

Chapter 2 - Concept and Principles of Privacy and Global Privacy Legislative Landscape

Chapter 3 - South African Privacy Legislation

Part 3 - Privacy Legislation Comparison

Chapter 4 - Extent to which the Privacy Legislation of the European Union and South Africa addresses the International 2013 OECD Guidelines

Part 4 - Proposed Framework

Chapter 5 - Proposed Framework with a Selection of Security Safeguards

Part 5 - Research Survey and Results

Chapter 6 - POPI Research Survey

Chapter 7 - Level of Compliance with the POPI Act and Specifically Condition 7 of the POPI Act

Chapter 8 - Current State of Security Safeguards and Validation of the Selection of Security Safeguards

Part 6 - Model of Operation of Security Safeguards

Chapter 9 - Model of Operation of Security Safeguards

Part 7 - Conclusion

Chapter 10 - Conclusion

8.1 INTRODUCTION

A framework to achieve and maintain compliance with Condition 7 of the Protection of Personal Information (POPI) Act, (Act 4 of 2013) was proposed in Chapter 5. The proposed POPI Condition 7 framework included a selection of security safeguards to ensure confidentiality and integrity of electronic personal information stored, processed or transmitted. Chapter 6 provided an overview of the research design, research instrumentation, research group, data analysis approach and assessed the demographics associated with the POPI research survey results in terms of a participant's institution. Chapter 7 presented the current level of compliance with the POPI Act (2013) and specifically Condition 7 of the Act as well as the financial value associated with electronic personal information and the potential impact of a data breach of electronic personal information. This chapter utilising the POPI research survey results from 167 participants addresses the following research questions:

- Research question 4 - *What is the current state of security safeguards within South African institutions to achieve compliance with Condition 7 of the POPI Act (2013), specifically in relation to electronic personal information?*
- Research question 5 - *To what extent is the selection of security safeguards proposed as part of the framework within this thesis valid?*

This chapter analyses the POPI research survey results in terms of the current state of security safeguards within South African institutions to achieve compliance with Condition 7 of the POPI Act (2013), specifically in relation to electronic personal information. This analysis is achieved by firstly, providing an overview of the selection of security safeguards across 3 domains (management, operational and technical) from several leading practices, as per the "Secure" phase of the proposed POPI Condition 7 framework in Chapter 5, to ensure the confidentiality and integrity of electronic personal information as required by Condition 7 of the POPI Act (2013). Secondly, the current state of security safeguards is assessed by exploring the applicability, extent of implementation and completeness of the selection of security safeguards. Applicability explores if the security safeguard is used within an institution. The extent of implementation assesses if the security safeguard is fully implemented, partially implemented or is being considered for implementation. Lastly, completeness assesses if there are any additional security safeguards, which may not have been considered to ensure confidentiality and integrity of electronic personal information as required by Condition 7 of the POPI Act (2013).

By obtaining an understanding of the current state of security safeguards the validity of the selection of security safeguards within the proposed POPI Condition 7 framework is also assessed. The applicability factor allows for the identification of security safeguards not utilised in South African institutions based on the POPI research survey results from the 167 participants. On the other hand, the completeness factor allows for the identification of security safeguards used within South African institutions, which were not considered as part of the "Secure" phase of the proposed POPI Condition 7 framework in the selection of security safeguards to ensure the confidentiality and integrity of electronic personal information.

Lastly, a critical evaluation in terms of key findings and recommendations based on the analysis of the POPI research survey results is provided.

8.2 SELECTION OF SECURITY SAFEGUARDS

In Chapter 5, the "Secure" phase of the proposed POPI Condition 7 framework encapsulates a selection of security safeguards across management, operational and technical domains, to facilitate the achievement and maintenance of compliance with Condition 7 of the POPI Act (2013), with a specific focus on preventing unauthorised disclosure (maintaining confidentiality) and modification (ensuring integrity) of electronic personal information stored, processed or transmitted. The management domain accounted for 5 security safeguards, namely information security governance, risk management, information security policy, supplier and service level management and business continuity management. This was followed by the operational domain which accounted for 6 security safeguards, namely security procedures and processes, baseline infrastructure security standards, security awareness and training, security monitoring, incident and reporting, security assessment and disaster recovery. The remaining 9 security safeguards formed part of the technical domain, namely network segmentation, encrypted data channels, server and network component security, workstation and laptop security, file integrity, firewalls, physical and environmental security, centralised audit logging, data loss prevention.

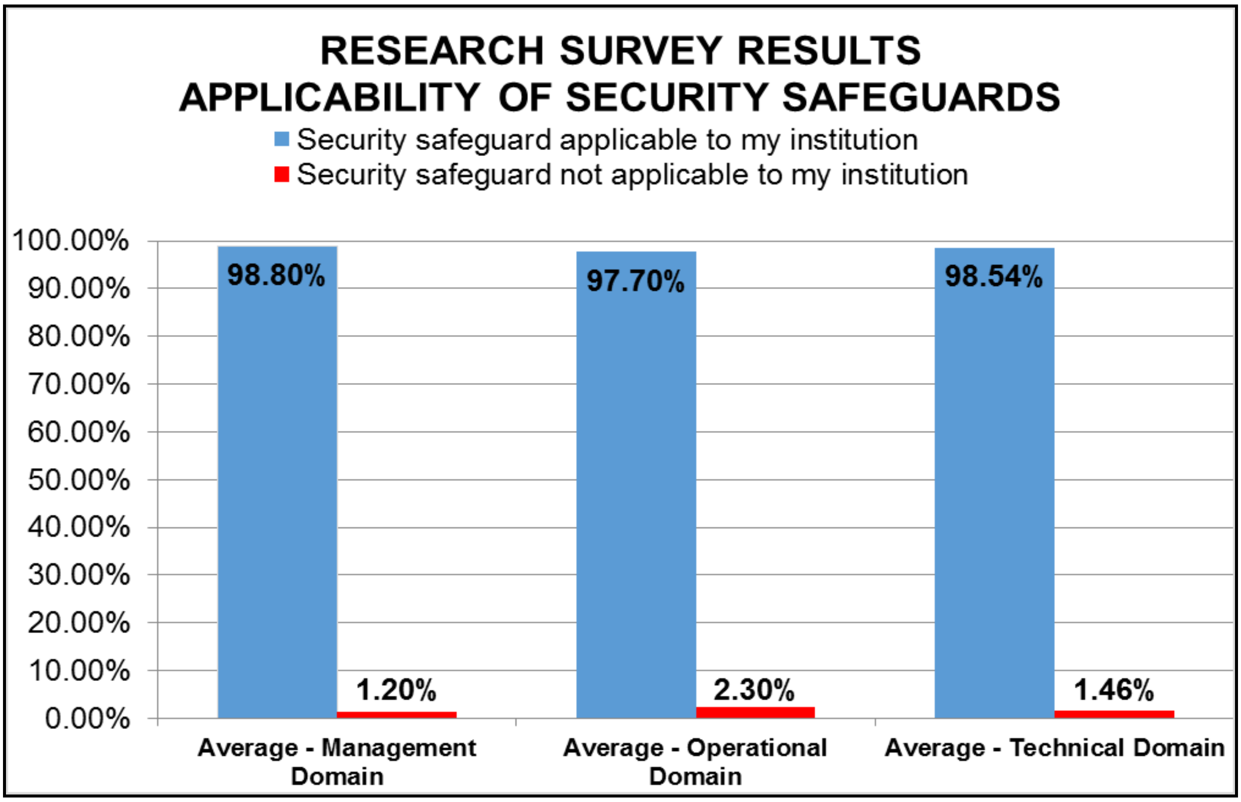
The aforementioned selection of security safeguards forms the basis for analysing the current state of security safeguards within South African institutions to achieve compliance with Condition 7 of the POPI Act (2013), specifically in relation to electronic personal information.

8.3 POPI Research Survey Results - Analysis

An analysis of the current state of security safeguards within South African institutions to achieve compliance with Condition 7 of the POPI Act (2013), specifically in relation to electronic personal information is provided from subsection 8.3.1 to 8.3.3 below. The analysis explores the applicability, extent of implementation and completeness of the selection of security safeguards based on the research survey responses received from the 167 participants who completed the POPI research survey.

8.3.1 Applicability of Security Safeguards

In terms of assessing the applicability of security safeguards, participants were asked if the security safeguards across the 3 domains were applicable (that is are the security safeguards within the 3 domains used within their institutions) or not applicable to their institutions, as it relates to ensuring the confidentiality and integrity of electronic personal information as required by Condition 7 of the POPI Act (2013), as illustrated in Figure 8.1 on the next page.



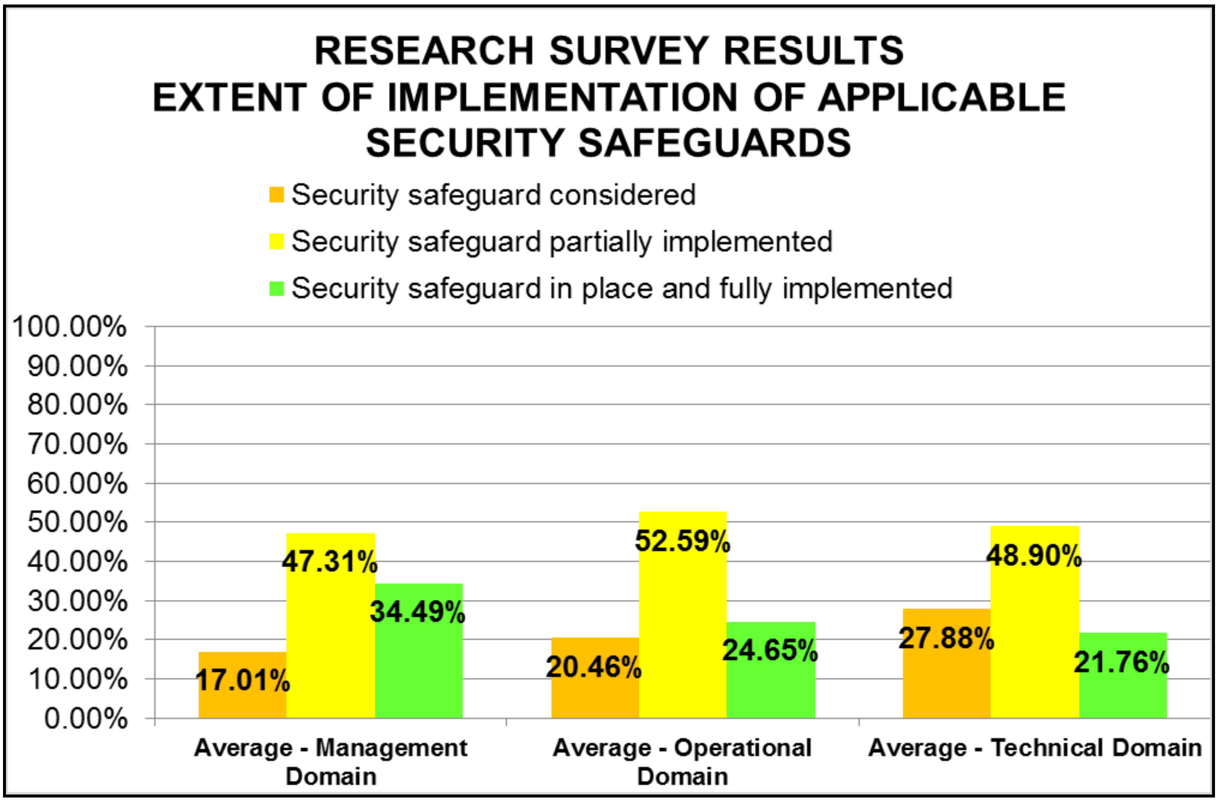
Security safeguard domain	Security safeguard applicable to my institution (response count)	Security safeguard applicable to my institution (response percentage)	Security safeguard not applicable to my institution (response count)	Security safeguard not applicable to my institution (response percentage)
Average - Management Domain	165.00	98.80%	2.00	1.20%
Average - Operational Domain	163.17	97.70%	3.83	2.30%
Average - Technical Domain	164.56	98.54%	2.44	1.46%
Overall Average - All Domains	**164.25**	**98.35%**	**2.75**	**1.65%**

Figure 8.1: Applicability of Security Safeguards

As per Figure 8.1 on the previous page, an average of 98.35% of participants stated that the security safeguards across the management, operational and technical domains were applicable to their respective institutions in that these are either being considered for implementation or already partially or fully implemented. However, an average of 1.65% participants stated that security safeguards across the management, operational and technical domains were not applicable to their respective institutions.

8.3.2 Extent of Implementation of Security Safeguards

The extent of implementation of the security safeguards across the 3 domains as illustrated in Figure 8.2 below is based on the average applicability of 98.35% associated with the security safeguards as per Figure 8.1 on the previous page. As such, the average extent of implementation of the security safeguards across the 3 domains is equivalent to 98.35% (22.93% of security safeguards considered for implementation, 49.61% of security safeguards partially implemented and 25.81% of security safeguards fully implemented, ultimately equating to a total of 98.35%).



Security safeguard domain	Security safeguard considered (response count)	Security safeguard considered (response percentage)	Security safeguard partially implemented (response count)	Security safeguard partially implemented (response percentage)	Security safeguard fully implemented (response count)	Security safeguard in place and fully implemented (response percentage)
Average - Management Domain	28.40	17.01%	79.00	47.31%	57.60	34.49%
Average - Operational Domain	34.17	20.46%	87.83	52.59%	41.17	24.65%
Average - Technical Domain	46.56	27.88%	81.67	48.90%	36.33	21.76%
Overall Average - All Domains	**38.30**	**22.93%**	**82.85**	**49.61%**	**43.10**	**25.81%**

Figure 8.2: Extent of Implementation of Applicable Security Safeguards

An average of 49.61% of participants, as per Figure 8.2 above, revealed partial implementation of the security safeguards across the 3 domains within their institutions. In addition, an average of 25.81% of participants stated that the security safeguards across the 3 domains were fully implemented in their institutions. However, an average of 22.93% of participants stated that the security safeguards across the 3 domains are still being considered within their institutions for implementation.

8.3.3 Completeness of Security Safeguards

To assess the completeness of security safeguards, the 167 participants were requested to assess if there are any additional security safeguards to the selection of security safeguards, which may not have been considered to ensure the confidentiality and integrity of electronic personal information as required by Condition 7 of the POPI Act (2013). 150 out of the 167 participants (89.8%) did not provide additional security safeguards that are being considered or implemented (partially or fully) by their institutions. However, 17 participants (10.2%) indicated that there were security safeguards that their institutions are considering or implementing (partially or fully) in addition to the selection of security safeguards proposed as part of the "Secure" phase of the proposed POPI Condition 7 framework in Chapter 5. From these 17 responses, 6 were invalid as they did not provide accurate and sufficient information for further consideration. However, the remaining 11 of the 17 responses, as listed in Table 8.1 below, provided accurate and sufficient information for further consideration.

Table 8.1: Security Safeguards Suggested by Participants

Number	Safeguards suggested by participants	Number	Safeguards suggested by participants
1	Database level encryption	7	Next generation firewall
2	Encryption	8	File integrity hashing value validation
3	Payment card industry data security standard (PCI DSS)	9	Firmware embedded basic input output system (BIOS) based persistent and remote asset tracking Data and device security
4	International standards and frameworks	10	We acquired an enterprise wide IT system to protect the electronic information
5	Security standards	11	Wi-Fi networks
6	Mobile device management		

An impact analysis of the 11 valid responses (Table 8.1 above) as depicted in Table 8.2 on the next page was conducted to assess the completeness of the selection of security safeguards as per the "Secure" phase of the proposed POPI Condition 7 framework in Chapter 5, to ensure confidentiality and integrity of electronic personal information. The impact analysis entailed grouping similar responses from the 11 valid responses and then assessing the responses in terms of either impacting or not impacting the selection of security safeguards as per the "Secure" phase of the proposed POPI Condition 7 framework in Chapter 5. A response was considered to impact the selection of security safeguards as per the "Secure" phase of the proposed POPI Condition 7 framework in Chapter 5, if it introduced new security safeguards or resulted in changes to the name of a security safeguard or an update of the description associated with a security safeguard. In comparison, a response was considered not to have an impact on the selection of security safeguards as per the proposed POPI Condition 7 framework in Chapter 5, if it resulted in no change at all as the current selection of security safeguards adequately address the information provided by a response. The result of the impact analysis for each grouping of responses was supported by a rationale. Furthermore, all responses considered to impact the selection of security safeguards as per the "Secure" phase of the proposed POPI Condition 7 framework in Chapter 5, was supported by a relevant action aimed at capturing the change required to the affected security safeguards.

Table 8.2: Impact Analysis of the Security Safeguards Suggested by Participants

Security safeguards suggested by participants	**Impact (Yes/No), rationale and action required (Yes/No)**
Response 1: Database level encryption ***Response 2:*** Encryption ***Response 9:*** Data security	***Impact (Yes/No):*** Yes - Current security safeguards (Encrypted data channels)
	Rationale: Encryption is only addressed from a data channel perspective by the encrypted data channels security safeguard.
	Action Required (Yes/No): Yes - Rename the "Encrypted data channels"security safeguard to "Encryption" and update the description to address encryption holistically from a data security perspective to cover data transmission (data channels) and storage (databases).
Response 3: Payment card industry data security standard (PCI-DSS)	***Impact (Yes/No):*** No
	Rationale: Credit card information is considered personal information however the Payment Card Industry - Data Security Standard (PCI-DSS) is a standard specifically for credit card information (PCI Security Standards Council, 2016) and does not apply to institutions who have personal information such as

Security safeguards suggested by participants	Impact (Yes/No), rationale and action required (Yes/No)
	names, surnames and email addresses of clients but no credit card information. As a result, PCI-DSS will not result in an additional security safeguard or an amendment to the security safeguards proposed. However, compliance with the PCI-DSS standard will encompass the implementation of the majority of the security safeguards proposed.
	Action Required (Yes/No): No
Response 4: International standards and frameworks ***Response 5:*** Security standards	***Impact (Yes/No):*** No
	Rationale: The baseline infrastructure security standards safeguard addresses security standards. Furthermore, the security safeguards includes the need for an information security policy, security procedures and processes as well as baseline infrastructure security standards, which should ideally be based on international standards and frameworks to prevent re-inventing the wheel. For example, the information security policy may be based on International Standards Organisation (ISO) 27001.
	Action Required (Yes/No): No
Response 6: Mobile device management ***Response 9:*** Device security	***Impact (Yes/No):*** Yes - Current security safeguards (workstation and laptop security as well as data loss prevention).
	Rationale: Workstation and laptop security makes no provision for mobile devices. Furthermore, data end points for data loss prevention are limited to workstations and laptops.
	Action Required (Yes/No): Yes **-** Rename the security safeguard “Workstation and laptop security” to “Workstation, laptop and mobile device security” and update the description of the security safeguard to include security of mobile devices. In addition,

Security safeguards suggested by participants	**Impact (Yes/No), rationale and action required (Yes/No)**
	update the description of the "Data loss prevention" security safeguard to include mobile devices as data end points.
Response 7: Next generation firewall	***Impact (Yes/No):*** Yes - Current security safeguards (file integrity).
	Rationale: Firewalls independent of vendor or technology is addressed by the current security safeguards (firewall).
	Action Required (Yes/No): No
Response 8: File integrity hashing value validation	***Impact (Yes/No):*** No
	Rationale: File integrity is addressed by the file integrity security safeguard, with no provision for hash value validation.
	Action Required (Yes/No): Yes - Update the description of the "File integrity" security safeguard to include hash value validation.
Response 9: Firmware embedded basic input output system (BIOS) based persistent and remote asset tracking	***Impact (Yes/No):*** Yes - Current security safeguards (Security monitoring, incident and reporting, workstation and laptop security as well as data loss prevention).
	Rationale: Yes - Security monitoring, incident and reporting safeguard as well as the workstation and laptop security and data loss prevention safeguards did not take into account asset tracking.
	Action Required (Yes/No): Yes - Update the description of the security monitoring, incident and reporting safeguard to include persistent and remote asset tracking. In addition, the workstation and laptop security safeguard description to be updated to include firmware BIOS based tracking on supported workstations, laptops and mobile devices. Furthermore, the data loss prevention safeguard to enable tracking of assets via data end

Security safeguards suggested by participants	**Impact (Yes/No), rationale and action required (Yes/No)**
	points, if firmware BIOS based asset tracking is not supported on workstations, laptops or mobile devices.
Response 10: We acquired an enterprise wide IT system to protect the electronic information	***Impact (Yes/No):*** No
	Rationale: Enterprise-wide IT system is open to interpretation and could be a data loss prevention (DLP) system or a security incident event and monitoring (SIEM) system. Both the DLP and SIEM systems are addressed by the current security safeguards (Data loss prevention and security monitoring, incident and reporting).
	Action Required (Yes/No): No
Response 11: Wi-Fi networks	***Impact (Yes/No):*** Yes - Current security safeguards (network segmentation as well as server and network component security).
	Rationale: The network segmentation as well as the server and network component security safeguards do not make a distinction between wired and wireless networks.
	Action Required (Yes/No): Yes - Update the description of the “Network segmentation” and “Server and network component security” safeguards to state that the security safeguards are applicable to any form of network may it be wired and wireless or a combination thereof.

As a result of the aforementioned impact analysis in Table 8.2 above, based on the 11 valid responses, 5 responses had no impact on the selection of security safeguards as per the “Secure” phase of the proposed POPI Condition 7 framework in Chapter 5, based on the rationale provided as part of the impact analysis in Table 8.2 above. However, 6 of the 11 valid responses had an impact on the selection of security safeguards as per the

“Secure” phase of the proposed POPI Condition 7 framework in Chapter 5, in that it resulted in updates to the security safeguards (name of the security safeguard or the description associated with the security safeguard), but no additional security safeguards were identified.

As a result of the aforementioned analysis relating to the completeness of the selection of security safeguards as well as the analysis relating to the applicability of the selection of security safeguards, the validity of the selection of security safeguards as per the “Secure” phase of the Proposed POPI Condition 7 framework may be assessed.

8.4 VALIDITY OF THE SELECTION OF SECURITY SAFEGUARD WITHIN THE PROPOSED POPI CONDITION 7 FRAMEWORK

The validity of the selection of security safeguards as per the “Secure” phase of the proposed POPI Condition 7 framework is dependent on the applicability and completeness factors associated with the current state of security safeguards within South African institutions to achieve compliance with Condition 7 of the POPI Act (2013), specifically in relation to electronic personal information.

The applicability factor allowed for the identification of security safeguards not utilised in South African institutions based on the POPI research survey results from the 167 participants. Table 8.3 on the next page illustrates the applicability of each of the 20 security safeguards which were proposed as per the “Secure” phase of the proposed POPI Condition 7 framework in Chapter 5.

Table 8.3: Applicability of the 20 Security Safeguards from the Proposed POPI Condition 7 Framework

Security safeguard	**Security safeguard not applicable to my institution (response count)**	**Security safeguard not applicable to my institution (response percentage)**	**Security safeguard applicable to my institution - under consideration, partially or fully implemented (response count)**	**Security safeguard applicable to my institution - under consideration, partially or fully implemented (response percentage)**
M1: Information Security Governance	0	0.00%	167	100.00%
M2: Risk Management	3	1.80%	164	98.20%
M3: Information Security Policy	1	0.60%	166	99.40%
M4: Supplier and Service Level Management	4	2.40%	163	97.60%
M5: Business Continuity Management	2	1.20%	165	98.80%
Average - Management Domain	**2.00**	**1.20%**	**165.00**	**98.80%**
O1: Security Procedures and Processes	3	1.80%	164	98.20%

Security safeguard	Security safeguard not applicable to my institution (response count)	Security safeguard not applicable to my institution (response percentage)	Security safeguard applicable to my institution - under consideration, partially or fully implemented (response count)	Security safeguard applicable to my institution - under consideration, partially or fully implemented (response percentage)
O2: Baseline Infrastructure Security Standards	3	1.80%	164	98.20%
O3: Security Awareness and Training	8	4.79%	159	95.21%
O4: Security Monitoring, Incident and Reporting	4	2.40%	163	97.60%
O5: Security Assessment	4	2.40%	163	97.60%
O6: Disaster Recovery	1	0.60%	166	99.40%
Average - Operational Domain	**3.83**	**2.30%**	**163.17**	**97.70%**
T1: Network Segmentation	1	0.60%	166	99.40%
T2: Encrypted Data Channels	3	1.80%	164	98.20%

Security safeguard	Security safeguard not applicable to my institution (response count)	Security safeguard not applicable to my institution (response percentage)	Security safeguard applicable to my institution - under consideration, partially or fully implemented (response count)	Security safeguard applicable to my institution - under consideration, partially or fully implemented (response percentage)
T3: Server and Network Component Security	2	1.20%	165	98.80%
T4: Workstation and Laptop Security	1	0.60%	166	99.40%
T5: File Integrity	5	2.99%	162	97.01%
T6: Firewalls	1	0.60%	166	99.40%
T7: Physical and Environmental Security	1	0.60%	166	99.40%
T8: Centralised Audit Logging	4	2.40%	163	97.60%
T9: Data Loss Prevention	4	2.40%	163	97.60%
Average - Technical Domain	**2.44**	**1.46%**	**164.56**	**98.54%**

All 20 security safeguards proposed as part of the “Secure” phase of the framework in Chapter 5 were considered to be applicable as each security safeguard on an individual basis was associated with an applicability factor, based on the number of responses received from participants, which exceeded 90%.

The completeness factor allows for the identification of security safeguards used within South African institutions, which were not considered as part of the “Secure” phase of the proposed POPI Condition 7 framework in the selection of security safeguards to ensure the confidentiality and integrity of electronic personal information. Based on the impact analysis in Table 8.2 within section 8.3.3 above as part of the completeness analysis, of the 11 valid responses, 5 responses had no impact on the security safeguards previously proposed as supported by the rationale provided. However, 6 of the 11 valid responses had an impact on the selection of security safeguards previously proposed, in that it did result in updates to the security safeguards (name of the security safeguard or the description associated with the security safeguard) but no additional security safeguards were identified.

As a result, the selection of security safeguards as per the “Secure” phase of the proposed POPI Condition 7 framework were valid given the level of applicability (each security safeguard proposed exceeded a 90% level of applicability) and completeness (there were updates to the name of the security safeguard or the description associated with the security safeguard, however no additional security safeguards were identified) associated with the selection of security safeguards.

8.5 Critical Evaluation - Key Findings and Recommendations

The analysis of the POPI research survey results forms the basis of the critical evaluation in terms of key findings and recommendations as it relates to the current state of security safeguards in terms of applicability, extent of implementation and completeness is provided from subsection 8.5.1 to 8.5.3 below. In addition, key findings and recommendations associated with the validity of the selection of security safeguards as per the “Secure” phase of the proposed POPI Condition 7 framework is provided in subsection 8.5.4.

8.5.1 Applicability of Security Safeguards

An average of 98.35% of participants stated that security safeguards across the management, operational and technical domains, as per the “Secure” phase of the proposed POPI Condition 7 framework, were applicable to their respective institutions (either being considered for implementation or already partially or fully implemented). An average of 1.65% of participants stated that security safeguards across the management, operational and technical domains were not applicable to their respective institutions. Certain security safeguards may not be applicable in the event where the institution has compensating safeguards (other alternative security safeguards to ensure confidentiality and integrity of electronic personal information) in place. However, in the event that the confidentiality and integrity of electronic personal information may be compromised due to the lack of a security safeguard, it is recommended that the security safeguards identified as not applicable to the institution across the management, operational and technical domains be re-considered for implementation to mitigate the risk of disclosure and modification of electronic personal information as well as to ultimately ensure compliance with Condition 7 of the POPI Act (2013).

8.5.2 Extent of Implementation of Security Safeguards

At the time of the POPI research survey being conducted an average of 25.81% of the 98.35% of participants stated that security safeguards across the management, operational and technical domains were fully implemented in their institution. However, security safeguards across the management, operational and technical domains were partially implemented (average of 49.61% of the 98.35% participants) or being considered for implementation (average of 22.93% of the 98.35% of participants). Given that the POPI Act (2013) is not yet enforceable, the progress made by South African institutions is considered acceptable in that the implementation of certain of the security safeguards account for a combined average of 75.42% of the 98.35% of participants (partial implementation - 49.61% and full implementation - 25.81%). South African institutions should aim to achieve full implementation of the security safeguards in order to contribute towards the achievement of ensuring compliance with Condition 7 of the POPI Act (2013) as well as the overall POPI Act (2013). As a result, the security safeguards that have been fully implemented can be continuously monitored to ensure that the confidentiality and integrity of electronic personal information is preserved, while the security safeguards that have been partially implemented should be fully implemented. Similarly, the security safeguards that are being considered for implementation should be prioritised and implemented in the most effective and efficient manner in order to achieve compliance with Condition 7 of the POPI Act (2013) as well as the overall Act.

8.5.3 Completeness of Security Safeguards

From a completeness perspective, no additional security safeguards were added to the selection of security safeguards as part of the "Secure" phase of the proposed POPI Condition 7 framework to ensure confidentiality and integrity of electronic personal information. However, based on the information provided by participants in terms of the responses received, driven by themes such as encryption, mobile devices and asset tracking, the names of 2 security safeguards (workstation and laptop security changed to workstation, laptop and mobile security as well as encrypted data channels changed to encryption) were updated. In addition, the description associated with 7 security safeguards was updated. The aforementioned updates are illustrated in italics within Table 8.4 below.

Table 8.4: Updates to the Security Safeguard Names and/or Descriptions

Update description	**Security safeguard name**	**Current safeguard description**	**Updated safeguard description**
Update to the security safeguard description	Security monitoring, incident and reporting	All audit logs from applications as well as the technology infrastructure is assessed in order to report on any malicious activities or	All audit logs from applications as well as the technology infrastructure is assessed in order to report on any malicious activities or data breaches of electronic personal

Update description	**Security safeguard name**	**Current safeguard description**	**Updated safeguard description**
		data breaches of electronic personal information.	information. ***Security monitoring to include persistent and remote asset tracking.***
Update to the security safeguard description	Network segmentation	Application and database servers that respectively process and store personal information are located on a dedicated network segment that is separated from the rest of the corporate network.	Application and database servers that respectively process and store personal information are located on a dedicated network segment ***(may be a wired or wireless network or a combination thereof)*** that is separated from the rest of the corporate network.
Update to the security safeguard name and description	***Encryption*** (previously encrypted data channels)	All electronic personal information flowing into and out of the dedicated network segment, is encrypted and access to the data channels is strictly monitored and controlled.	All electronic personal information ***transmitted*** (flowing into and out of the dedicated network segment) ***and stored***, is encrypted and access to the data channels and ***storage (databases)*** is strictly monitored and controlled.
Update to the	Server and	All server and network	All server and network

Update description	**Security safeguard name**	**Current safeguard description**	**Updated safeguard description**
security safeguard description	network component security	components are configured to implement the defined baseline infrastructure security standards.	(***may be a wired or wireless network or a combination thereof)*** components are configured to implement the defined baseline infrastructure security standards.
Update to the security safeguard name and description	***Workstation, laptop and mobile security*** (previously workstation and laptop security)	Workstations and laptops are configured to implement the defined baseline infrastructure security standards and are locked down to prevent the user to change the configuration or install additional applications.	Workstations, laptops and ***mobile devices*** are configured to implement the defined baseline infrastructure security standards and are locked down to prevent the user to change the configuration or install additional applications. ***In addition, firmware basic input output system (BIOS) based tracking should be enabled on supported workstations, laptops and mobile devices (for non-supported workstations, laptops and mobile***

Update description	**Security safeguard name**	**Current safeguard description**	**Updated safeguard description**
			devices asset tracking should be implemented through the data loss prevention security safeguard)
Update to the security safeguard description	File integrity	All configurations associated with server and network components are associated with a unique value known as a hash value. The hash value may be used to ascertain if unauthorised changes were affected to configurations.	All configurations associated with server and network components are associated with a unique value known as a hash value. The hash value may be used to ascertain if unauthorised changes were affected to configurations ***via hash value validation.***
Update to the security safeguard description	Data loss prevention	The protection of data loss for data at rest, in motion or at an end point. To prevent the loss of electronic personal information specifically via workstations or laptops.	The protection of data loss for data at rest, in motion or at an end point. To prevent the loss of electronic personal information specifically via workstations, laptops ***and mobile devices***. ***Furthermore, track assets via data end***

Update description	Security safeguard name	Current safeguard description	Updated safeguard description
			points, if firmware basic input output system (BIOS) based asset tracking (Workstation, laptop and mobile security safeguard) is not supported on workstations, laptops or mobile devices.

The model of operation of security safeguards which follows this chapter is based on the updates to the security safeguard names and descriptions as reflected in Table 8.4 above.

8.5.4 Validation of the Selection of Security Safeguards

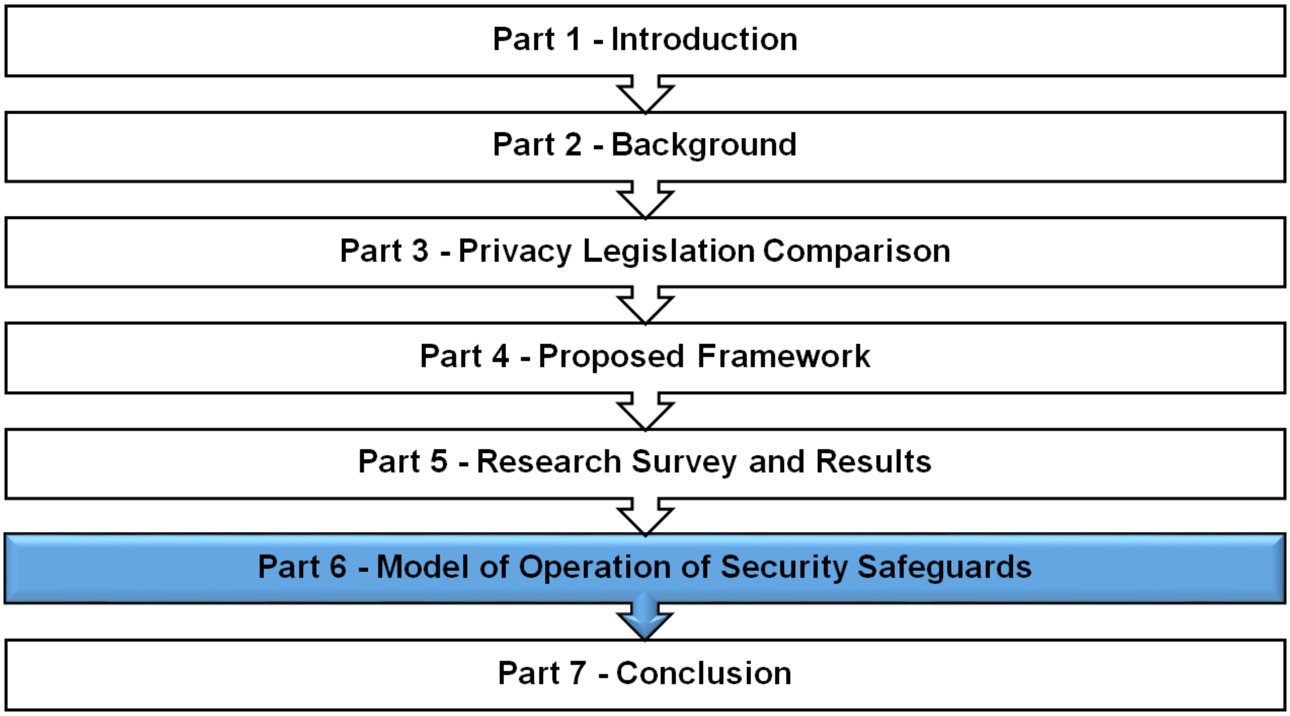
The selection of security safeguards within the “Secure” phase of the proposed POPI Condition 7 framework were valid given the level of applicability (each security safeguard proposed exceeded a 90% level of applicability) and completeness (there were updates to the name of the security safeguard or the description associated with the security safeguard, however no additional security safeguards were identified) associated with the selection of security safeguards. Therefore, it is recommended that the proposed POPI Condition 7 framework, which includes a validated selection of security safeguards as part of the “Secure” phase, be used by South African institutions to ultimately address the requirements of Condition 7 of the POPI Act (2013), specifically in relation to electronic personal information.

8.6 Conclusion

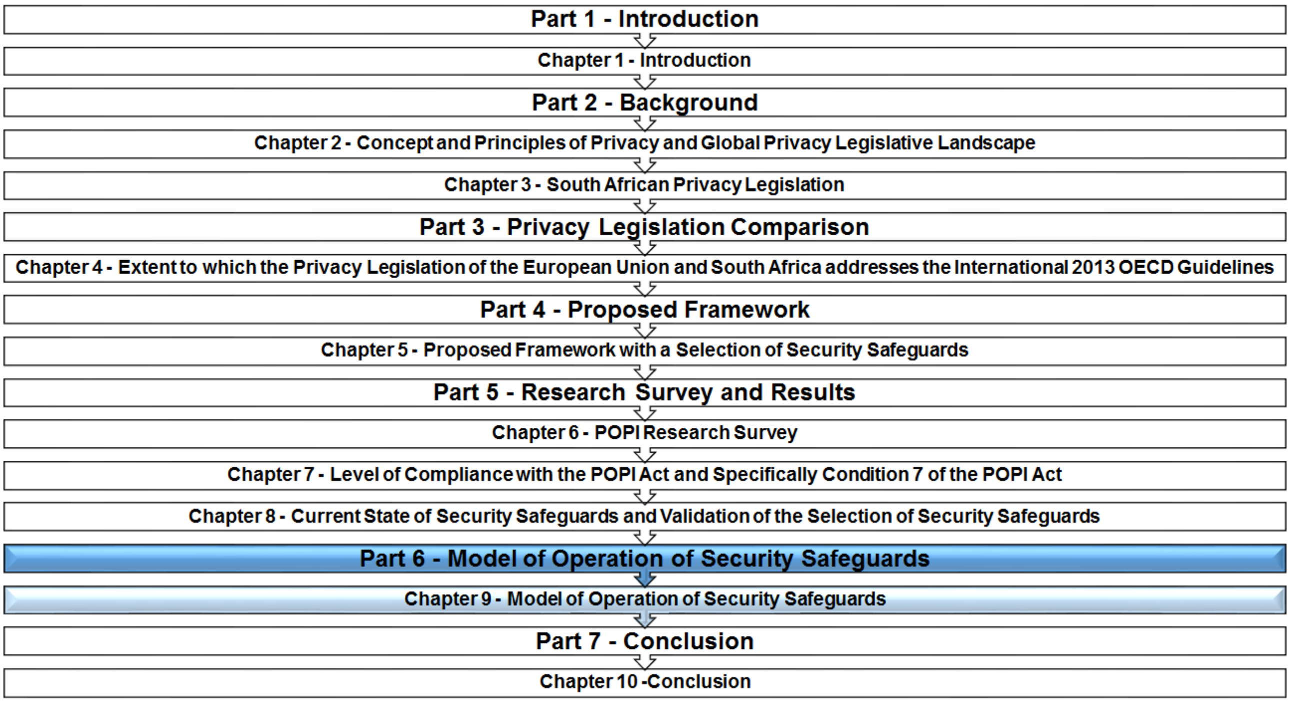
This chapter concluded Part 5 (Research Survey and Results) of this thesis by presenting an analysis of the current state of security safeguards within South African institutions to achieve compliance with Condition 7 of the POPI Act (2013), specifically in relation to electronic personal information. This analysis was achieved by firstly, providing an overview of the selection of security safeguards across 3 domains (management, operational and technical) from several leading practices, as per the “Secure” phase of the proposed POPI Condition 7 framework in Chapter 5, to ensure confidentiality and integrity of electronic personal information as required by Condition 7 of the POPI Act (2013). Secondly, research question 4 was addressed by assessing the current state of security safeguards through exploring the applicability, extent of implementation and completeness associated with the selection of security safeguards. In addition, research question 5 was addressed by assessing the validity of the selection of security safeguards as per the “Secure” phase of the proposed POPI Condition 7 framework. Lastly, a critical evaluation in terms of key findings and recommendations based on the analysis of the POPI research survey results was provided.

The updates to the selection of security safeguards identified in this chapter forms the basis of Part 6 (Model of Operation of Security Safeguards) of this thesis, in Chapter 9.

PART 6 - MODEL OF OPERATION OF SECURITY SAFEGUARDS


Part 1 - Introduction
Part 2 - Background
Part 3 - Privacy Legislation Comparison
Part 4 - Proposed Framework
Part 5 - Research Survey and Results
Part 6 - Model of Operation of Security Safeguards
Part 7 - Conclusion

CHAPTER 9 - MODEL OF OPERATION OF SECURITY SAFEGUARDS



Part 1 - Introduction
Chapter 1 - Introduction
Part 2 - Background
Chapter 2 - Concept and Principles of Privacy and Global Privacy Legislative Landscape
Chapter 3 - South African Privacy Legislation
Part 3 - Privacy Legislation Comparison
Chapter 4 - Extent to which the Privacy Legislation of the European Union and South Africa addresses the International 2013 OECD Guidelines
Part 4 - Proposed Framework
Chapter 5 - Proposed Framework with a Selection of Security Safeguards
Part 5 - Research Survey and Results
Chapter 6 - POPI Research Survey
Chapter 7 - Level of Compliance with the POPI Act and Specifically Condition 7 of the POPI Act
Chapter 8 - Current State of Security Safeguards and Validation of the Selection of Security Safeguards
Part 6 - Model of Operation of Security Safeguards
Chapter 9 - Model of Operation of Security Safeguards
Part 7 - Conclusion
Chapter 10 -Conclusion

9.1 INTRODUCTION

Chapter 8 provided the current state of security safeguards within South African institutions to achieve compliance with Condition 7 of the Protection of Personal Information (POPI) Act, (Act 4 of 2013), specifically in relation to electronic personal information. In addition, the validity of the selection of security safeguards proposed as part of the proposed POPI Condition 7 framework within Chapter 5 was also assessed. This chapter addresses research question 6 - *How can the security safeguards proposed as part of the framework within this thesis be implemented to achieve and maintain confidentiality and integrity of electronic personal information as required by Condition 7 of the POPI Act (2013)?*

This chapter proposes a model of operation of security safeguards to guide one on how the selection of security safeguards should be implemented to achieve and maintain confidentiality and integrity of electronic personal information as required by Condition 7 of the POPI Act (2013). This includes an overview of the revised selection of security safeguards which forms the basis for the model of operation of security safeguards. In addition, the prerequisites applicable to the model of operation of security safeguards are provided. Lastly, this chapter provides the benefits and limitations associated with the model of operation of security safeguards as part of a critical evaluation.

9.2 REVISED SELECTION OF SECURITY SAFEGUARDS

In Chapter 8, the validity of the selection of security safeguards as per the "Secure" phase of the proposed POPI Condition 7 framework was assessed. This assessment revealed that the selection of security safeguards within the proposed POPI Condition 7 framework were valid given the level of applicability (each security safeguard proposed exceeded a 90% level of applicability) and completeness (updates to the names and descriptions of certain security safeguards but no additional security safeguards were identified) associated with the selection of security safeguards. As such, Table 9.1 on the next page provides the revised selection of security safeguards (updates highlighted in italics) applicable to the model of operation of security safeguards to be considered for implementation to achieve and maintain the confidentiality and integrity of electronic personal information as required by Condition 7 of the POPI Act (2013).

Table 9.1: Revised Selection of Security Safeguards

Number	Security safeguard name	Security safeguard description
Management domain		
1	M1: Information Security Governance	Leadership, organisational structures as well as clear roles and responsibilities (ISACA, 2006 and ISO, 2013) for safeguarding electronic personal information.
2	M2: Risk Management	Governance, evaluation and a response to risks presented by electronic personal information (ISACA, 2009 and 2014c).
3	M3: Information Security Policy	Management direction and support for information security to be achieved through a formally defined and approved information security policy (ISO, 2013).
4	M4: Supplier and Service Level Management	Contracts in place with third party operators external to the institution as well as internal stakeholders within the institution responsible for providing services in relation to electronic personal information (ISACA, 2014c and OGCUK, 2007a).
5	M5: Business Continuity Management	The ability to recover from a business interruption in the most effective and efficient manner (Drewitt, 2013, ISACA, 2014c, ISO 2012 and 2013), which includes the recovery of electronic personal information maintained by an institution.
Operational domain		
6	O1: Security Procedures and Processes	Security procedures and processes in place to maintain the confidentiality and integrity of electronic personal information. The security procedure and process areas

Number	Security safeguard name	Security safeguard description
		to be considered include: change and configuration management, patch management, availability management, incident management, backup management, user account and access management (ISACA, 2014c, ISO, 2013 and OGCUK, 2007b) as well as the management of encryption keys to secure data channels (BSI, 2005).
7	O2: Baseline Infrastructure Security Standards	All server, workstation and laptop operating systems, database servers, web servers, network components (firewalls, routers, wireless) that form part of the technology infrastructure, to enable the protection of electronic personal information, should apply baseline infrastructure security standards as a security safeguard to prevent the adoption of default configurations and to ensure consistent configurations (NIST, 2013).
8	O3: Security Awareness and Training	Employees, contractors or third party operators need to be provided with awareness and training with regards to information security (ISO, 2013, NIST, 2013 and OGCUK, 2007b), with a specific focus on the security of electronic personal information.
9	O4: Security Monitoring, Incident and Reporting	All audit logs from applications as well as the technology infrastructure is assessed in order to report on any malicious activities or data breaches of electronic personal information (ISACA, 2014c, NIST, 2013 and OGCUK, 2007b). ***Security monitoring to include persistent and remote asset tracking.***
10	O5: Security Assessment	Regular security assessments to be performed in order to assess the security posture of the institution from a technical, organisational, procedural, administrative or

Number	Security safeguard name	Security safeguard description
		physical security perspective (NIST, 2013 and Palmer et al., 2001).
11	O6: Disaster Recovery	People, processes and technology associated with the storage, processing and transmission of electronic personal information to ensure continued operations to be defined (Drewitt, 2013, ISO 2012 and 2013, and NIST 2013).
Technical domain		
12	T1: Network Segmentation	Application and database servers that respectively process and store personal information are located on a dedicated network segment ***(may be a wired or wireless network or a combination thereof)*** that is separated from the rest of the corporate network (NIST, 2013).
13	***T2: Encryption*** (previously encrypted data channels)	All electronic personal information ***transmitted*** (flowing into and out of the dedicated network segment) ***and stored***, is encrypted and access to the data channels and ***storage (databases)*** is strictly monitored and controlled (ISO, 2013 and NIST, 2013).
14	T3: Server and Network Component Security	All server and network (***may be a wired or wireless network or a combination thereof)*** components are configured to implement the defined baseline infrastructure security standards (ISACA, 2014c and NIST, 2013).
15	***T4: Workstation, Laptop and Mobile Security*** (previously workstation and	Workstations, laptops and ***mobile devices*** are configured to implement the defined baseline infrastructure security standards and are locked down to prevent the user to change the configuration or install additional applications (ISACA, 2014c and NIST, 2013).

Number	Security safeguard name	Security safeguard description
	laptop security)	***In addition, firmware basic input output system (BIOS) based tracking should be enabled on supported workstations, laptops and mobile devices (for non-supported workstations, laptops and mobile devices asset tracking should be implemented through the data loss prevention security safeguard)***.
16	T5: File Integrity	All configurations associated with server and network components are associated with a unique value known as a hash value (ISACA, 2014c and OGCUK, 2007b). The hash value may be used to ascertain if unauthorised changes were affected to configurations ***via hash value validation.***
17	T6: Firewalls	A firewall should be used to separate the application and database servers that respectively process and store electronic personal information located on a dedicated network segment from the rest of the corporate network (NIST, 2013).
18	T7: Physical and Environmental Security	Physical and environmental security safeguards in place within the server rooms hosting the applications as well as the technology infrastructure associated with the storage, processing and transmission of electronic personal information. Physical security safeguards to control access to the server rooms and environmental security safeguards to provide alternate power sources to ensure availability as well as to protect against environmental hazards such as floods and fire should be in place (ISACA, 2014c, ISO, 2013 and NIST, 2013).
19	T8: Centralised	Audit logs to be maintained for all applications as well as the technology infrastructure associated with storing,

Number	Security safeguard name	Security safeguard description
	Audit Logging	processing and transmitting electronic personal information. All the audit logs maintained should be sent to a centralised audit logging server where analysis may be performed to identify ineffective security safeguards as well as security incidents and to serve as the basis for conducting an investigation in the event of a data breach of electronic personal information (ISACA, 2014c, ISO, 2013 and NIST, 2013).
20	T9: Data Loss Prevention	The protection of data loss for data at rest, in motion or at an end point. To prevent the loss of electronic personal information specifically via workstations, laptops ***and mobile devices*** (ISACA 2014b, ISO 2012 and NIST 2013). ***Furthermore, track assets via data end points, if firmware basic input output system (BIOS) based asset tracking (Workstation, laptop and mobile security safeguard) is not supported on workstations, laptops or mobile devices.***

The revised selection of security safeguards as per Table 9.1 above, to be considered for implementation to achieve and maintain the confidentiality and integrity of electronic personal information as required by Condition 7 of the POPI Act (2013) forms the basis for the model of operation of security safeguards. In addition, the implementation of the model of operation of security safeguards is associated with a prerequisite in the form of the identification of electronic personal information.

9.3 Prerequisites Applicable to the Model of Operation of Security Safeguards

In order to ensure the confidentiality and integrity of electronic personal information the identification of such information is required based on where it is stored, processed and transmitted within an institution, as per the “Identify” phase of the proposed POPI Condition 7 framework. This creates a platform for selecting and implementing the appropriate security safeguards from Table 9.1 above, to ultimately ensure confidentiality and integrity of electronic personal information. Therefore, the identification of electronic personal information is a prerequisite applicable to the implementation of the model of operation of security safeguards.

This prerequisite may be achieved by the process highlighted in Figure 9.1 below, which entails locating all the business processes in the institution associated with electronic personal information. Within each business process the information assets which store, process and transmit electronic personal information should be determined. This will result in the identification of all the input, processing and storage information assets such as web sites or mobile applications, applications and databases. Each storage information asset (database) identified should be queried to confirm the electronic personal information stored by the institution as well as to confirm the source of the electronic personal information in terms of the associated processing information asset (application) to which the data storage information asset (database) is linked as well as the data channels for transmission of electronic personal information between the web site or mobile application, application and database. Thereafter, the platform for applying the model of operation of safeguards is in place to ultimately ensure confidentiality and integrity of electronic personal information.

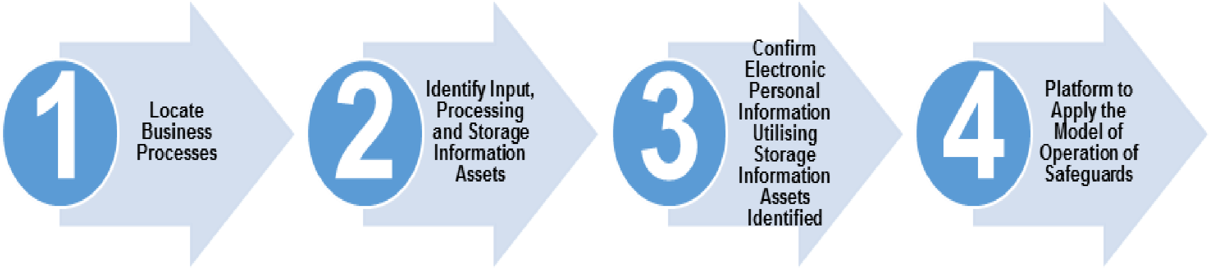

1
Locate Business Processes
2
Identify Input, Processing and Storage Information Assets
3
Confirm Electronic Personal Information Utilising Storage Information Assets Identified
4
Platform to Apply the Model of Operation of Safeguards

Figure 9.1: Prerequisite Electronic Personal Information Identification Process

By way of example, as illustrated in Figure 9.2 below, the prerequisite electronic personal information identification process is applied to a customer business process whereby a customer enters electronic personal information such as for example, their name, address, identity number and contact details via a web site.

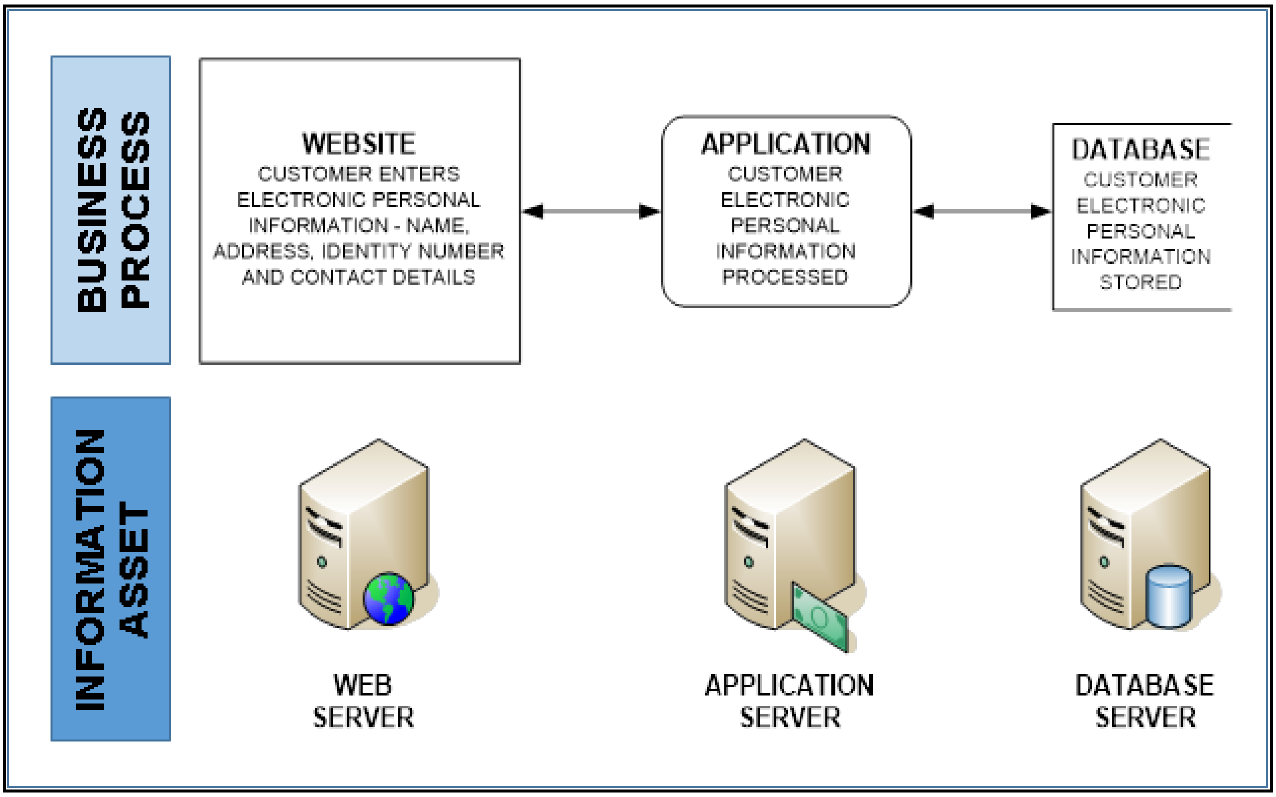

BUSINESS PROCESS
WEBSITE
CUSTOMER ENTERS ELECTRONIC PERSONAL INFORMATION - NAME, ADDRESS, IDENTITY NUMBER AND CONTACT DETAILS
APPLICATION
CUSTOMER ELECTRONIC PERSONAL INFORMATION PROCESSED
DATABASE
CUSTOMER ELECTRONIC PERSONAL INFORMATION STORED
INFORMATION ASSET
WEB SERVER
APPLICATION SERVER
DATABASE SERVER

Figure 9.2: Customer Business Process and Corresponding Information Assets

The electronic personal information provided by the customer captured via the web site is transmitted to the application, which in turn stores it in a database. Therefore, the input information asset is the web server hosting the web site and the processing information asset is the application server and the storage information asset is the database server. The database should then be queried to ensure that the name, address, identity number and contact details electronic personal information is stored. In so doing, the number of customer records may also be determined. Lastly, the data source of the electronic personal information stored in the database should be confirmed to the associated application and the data channels which enable the transmission of electronic personal information between the web site, application and database should also be confirmed.

This should result in a mapping of the all the input, processing and storage information assets as well as the data channels associated with electronic personal information as illustrated in Table 9.2 below, based on the aforementioned example.

Table 9.2: Mapping of Input, Processing and Storage Information Assets and Data Channels Associated with Electronic Personal Information

Business process	Input information asset	Processing information asset	Storage information asset	Data channels
Customer	Web Server	Application Server	Database Server	Web Server to/from Application Server Application Server to/from Database Server

Once the mapping of the all the input, processing and storage information assets as well as the data channels associated with electronic personal information is complete, the model of operation of safeguards may be applied by selecting and implementing appropriate safeguards to the identified information assets in order to ultimately ensure confidentiality and integrity of electronic personal information.

9.4 Model of Operation of Security Safeguards

In order to address the research question associated with this chapter a model of operation of security safeguards is proposed, as illustrated in Figure 9.3 on the next page. This model of operation of security safeguards demonstrates how the selection of security safeguards as per section 9.2 of this chapter should be implemented to achieve and maintain confidentiality and integrity of electronic personal information as required by Condition 7 of the POPI Act (2013).

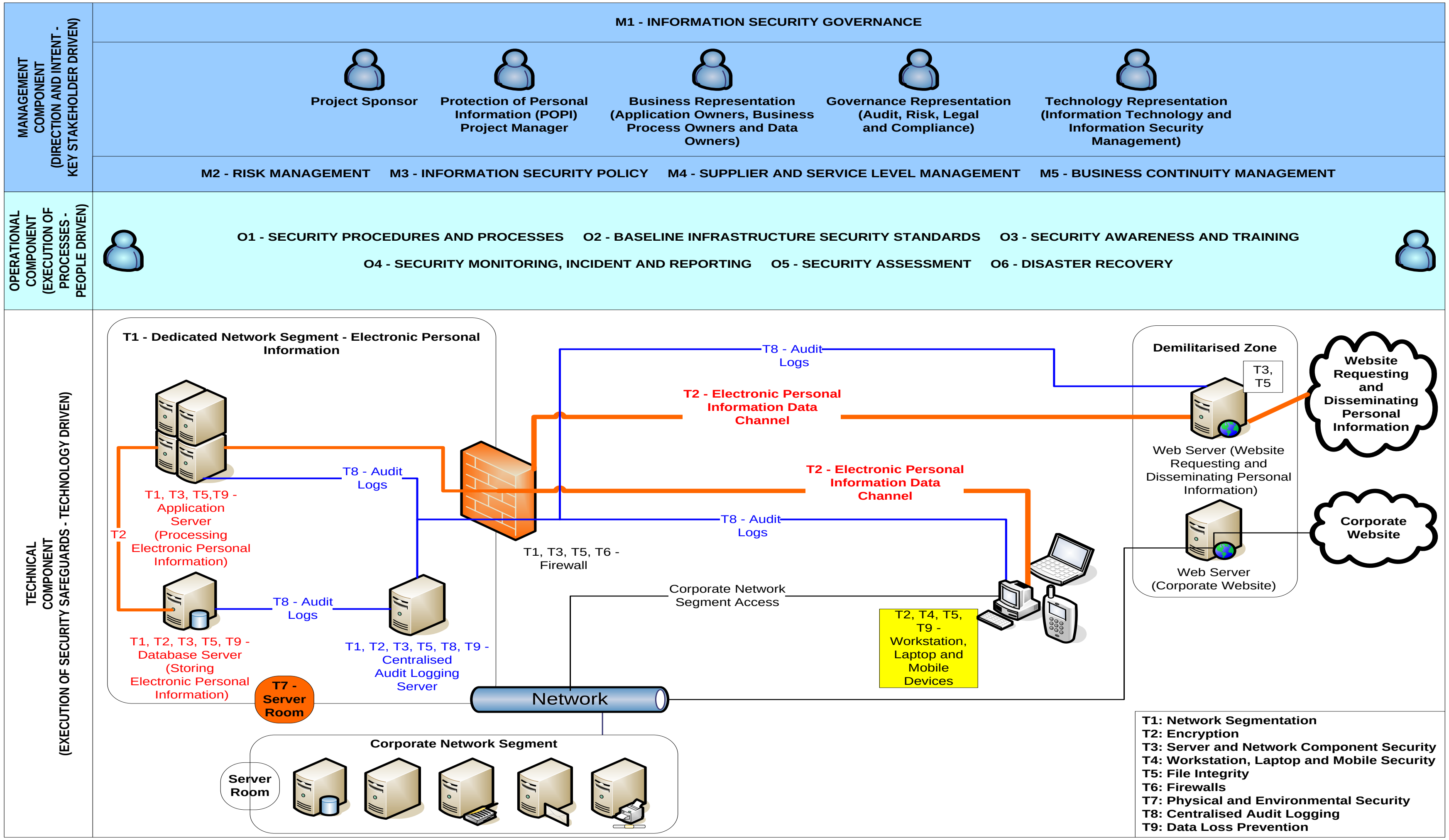

MANAGEMENT COMPONENT (DIRECTION AND INTENT - KEY STAKEHOLDER DRIVEN)
M1 - INFORMATION SECURITY GOVERNANCE
Project Sponsor
Protection of Personal Information (POPI) Project Manager
Business Representation (Application Owners, Business Process Owners and Data Owners)
Governance Representation (Audit, Risk, Legal and Compliance)
Technology Representation (Information Technology and Information Security Management)
M2 - RISK MANAGEMENT
M3 - INFORMATION SECURITY POLICY
M4 - SUPPLIER AND SERVICE LEVEL MANAGEMENT
M5 - BUSINESS CONTINUITY MANAGEMENT
OPERATIONAL COMPONENT (EXECUTION OF PROCESSES - PEOPLE DRIVEN)
O1 - SECURITY PROCEDURES AND PROCESSES
O2 - BASELINE INFRASTRUCTURE SECURITY STANDARDS
O3 - SECURITY AWARENESS AND TRAINING
O4 - SECURITY MONITORING, INCIDENT AND REPORTING
O5 - SECURITY ASSESSMENT
O6 - DISASTER RECOVERY
TECHNICAL COMPONENT (EXECUTION OF SECURITY SAFEGUARDS - TECHNOLOGY DRIVEN)
T1 - Dedicated Network Segment - Electronic Personal Information
T1, T3, T5,T9 - Application Server (Processing Electronic Personal Information)
T2
T8 - Audit Logs
T1, T2, T3, T5, T9 - Database Server (Storing Electronic Personal Information)
T8 - Audit Logs
T1, T2, T3, T5, T8, T9 - Centralised Audit Logging Server
T7 - Server Room
T1, T3, T5, T6 - Firewall
T8 - Audit Logs
T2 - Electronic Personal Information Data Channel
T2 - Electronic Personal Information Data Channel
T8 - Audit Logs
Corporate Network Segment Access
T2, T4, T5, T9 - Workstation, Laptop and Mobile Devices
Network
Corporate Network Segment
Server Room
Demilitarised Zone
T3, T5
Web Server (Website Requesting and Disseminating Personal Information)
Website Requesting and Disseminating Personal Information
Web Server (Corporate Website)
Corporate Website
T1: Network Segmentation
T2: Encryption
T3: Server and Network Component Security
T4: Workstation, Laptop and Mobile Security
T5: File Integrity
T6: Firewalls
T7: Physical and Environmental Security
T8: Centralised Audit Logging
T9: Data Loss Prevention

Figure 9.3: Model of Operation of Security Safeguards

The model of operation of security safeguards consists of 3 components based on the 3 domains associated with the selection of security safeguards as per the "Secure" phase of the proposed POPI Condition 7 framework, namely the management component, operational component and technical component. These components are aligned to the management, operational and technical domains of the selection of security safeguards as per the "Secure" phase of the proposed POPI Condition 7 framework, as illustrated in Table 9.3 below, since the functionality of each component is dependent on the selection of security safeguards in the respective domain.

Table 9.3: Alignment between Components of the Model of Operation of Security Safeguards and the Security Safeguard Domains

Components of the model of operation of safeguards	**Security safeguard domains**
Management Component	Management Domain
Operational Component	Operational Domain
Technical Component	Technical Domain

The management component of the model of operation of security safeguards is associated with the 5 security safeguards in the management domain as listed in section 9.2 of this chapter. Similarly, the operational and technical components of the model of operation of security safeguards are associated with 6 and 11 security safeguards in the operational and technical domains respectively, as listed in section 9.2 of this chapter.

These components of the model of operation of security safeguards are discussed from section 9.4.1 to 9.4.3 which follows below.

9.4.1 MANAGEMENT COMPONENT

The management component of the model of operation of security safeguards is associated with 5 security safeguards, as illustrated in Figure 9.4 on the next page, is driven from a key stakeholder perspective to provide direction and demonstrate intent to achieve and maintain compliance with the POPI Act (2013).

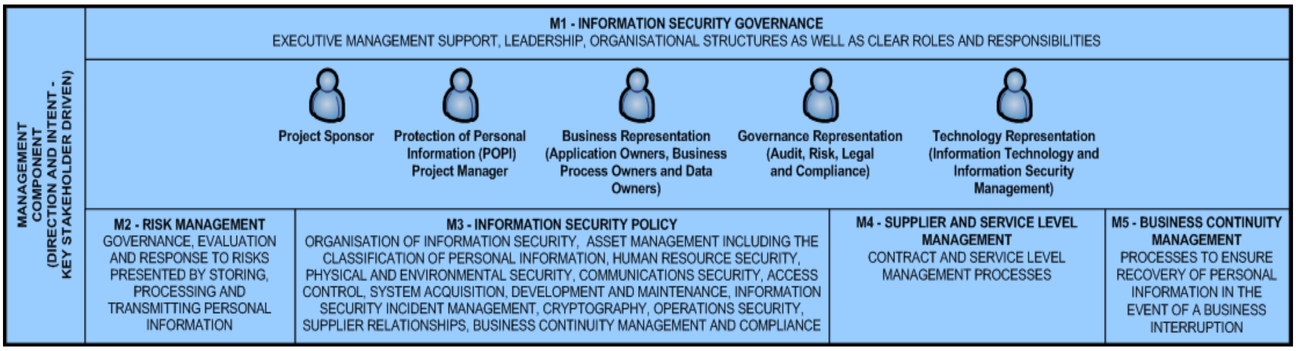

MANAGEMENT COMPONENT (DIRECTION AND INTENT - KEY STAKEHOLDER DRIVEN)
M1 - INFORMATION SECURITY GOVERNANCE
EXECUTIVE MANAGEMENT SUPPORT, LEADERSHIP, ORGANISATIONAL STRUCTURES AS WELL AS CLEAR ROLES AND RESPONSIBILITIES
Project Sponsor
Protection of Personal Information (POPI) Project Manager
Business Representation (Application Owners, Business Process Owners and Data Owners)
Governance Representation (Audit, Risk, Legal and Compliance)
Technology Representation (Information Technology and Information Security Management)
M2 - RISK MANAGEMENT
GOVERNANCE, EVALUATION AND RESPONSE TO RISKS PRESENTED BY STORING, PROCESSING AND TRANSMITTING PERSONAL INFORMATION
M3 - INFORMATION SECURITY POLICY
ORGANISATION OF INFORMATION SECURITY, ASSET MANAGEMENT INCLUDING THE CLASSIFICATION OF PERSONAL INFORMATION, HUMAN RESOURCE SECURITY, PHYSICAL AND ENVIRONMENTAL SECURITY, COMMUNICATIONS SECURITY, ACCESS CONTROL, SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE, INFORMATION SECURITY INCIDENT MANAGEMENT, CRYPTOGRAPHY, OPERATIONS SECURITY, SUPPLIER RELATIONSHIPS, BUSINESS CONTINUITY MANAGEMENT AND COMPLIANCE
M4 - SUPPLIER AND SERVICE LEVEL MANAGEMENT
CONTRACT AND SERVICE LEVEL MANAGEMENT PROCESSES
M5 - BUSINESS CONTINUITY MANAGEMENT
PROCESSES TO ENSURE RECOVERY OF PERSONAL INFORMATION IN THE EVENT OF A BUSINESS INTERRUPTION

Figure 9.4: Model of Operation of Security Safeguards - Management Component

Key stakeholders should include, but are not limited to, the project sponsor, project manager/information officer as well as representation from a business, governance and technology. The project sponsor of the POPI project should be responsible for providing strategic direction, support, funding and holding key stakeholders accountable to ensure and maintain compliance with the POPI Act (2013). The POPI project manager/information officer will firstly, drive the initiative to ensure compliance with the POPI Act (2013) and thereafter should be responsible for maintaining compliance with the Act. Business representation is critical in the form of application owners, business process owners and data owners as they would all play a critical role in the identification of personal information within the institution and ensure the compliance with the POPI Act (2013) during the execution of day-to-day activities. Governance representation in the form of audit, risk, legal and compliance will play a pivotal role in providing independent assurance in terms of the extent of compliance with the POPI Act (2013) as the initiative to ensure compliance is underway (audit function). Thereafter, the compliance function will monitor compliance to ensure that the institution is indeed complying with the POPI Act (2013) and the risk management function will manage the non-compliance risk and while the legal function will address legal matters that may arise due to non-compliance with the POPI Act (2013). Technology representation in the form of information technology and information security management will be responsible for the definition, execution and monitoring of processes within the operational domain (information security management) as well as the technology required to implement the security safeguards in the technical domain (information technology management).

As illustrated in Figure 9.4 on the previous page, the management component of the model of operation of security safeguards is associated with 5 security safeguards. In terms of the *M1: Information Security Governance* security safeguard executive management support and leadership is required to drive the POPI compliance initiative. In addition, the organisational structures such as a formal steering committee to oversee the POPI compliance initiative as well as clear roles and responsibilities for safeguarding electronic personal information need to be defined.

This is followed by the *M2: Risk Management* security safeguard which requires the governance, evaluation and a response to risks presented by storing, processing and transmitting electronic personal information that may lead to non-compliance with the POPI Act (2013). This may form part of the overall enterprise wide risk management processes and the risk register of the institution should include risks relating to the storage, processing and transmission of electronic personal information.

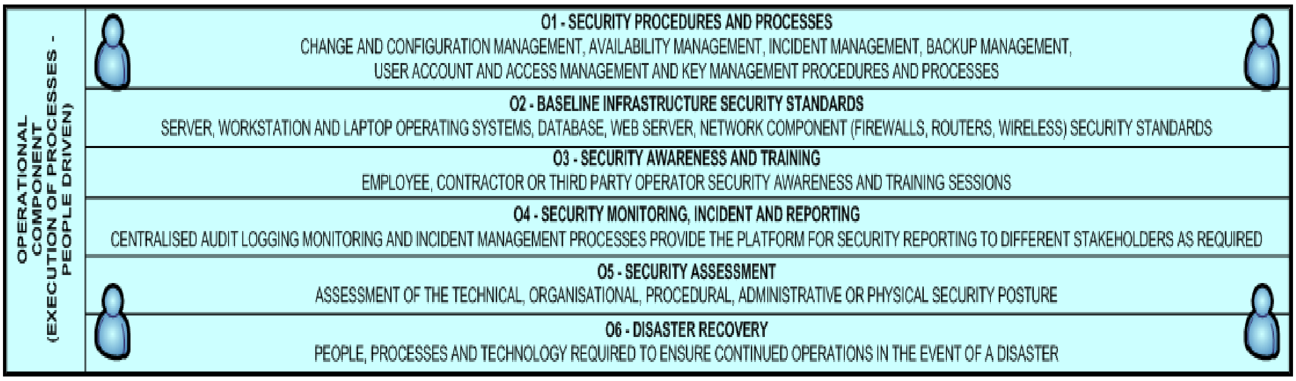
The *M3: Information Security Policy* security safeguard requires a formally defined, approved and implemented information security policy addressing the confidentiality and integrity of electronic personal information as it relates to the organisation of information security, asset management, human resource security, physical and environmental security, communication security, access control, system acquisition, development and maintenance, information security incident management, cryptography, operations security, supplier relationships, business continuity management and compliance.

The next security safeguard is *M4: Supplier and Service Level Management* where contract and service level management processes are applied to third party contractors external to the institution as well as internal stakeholders within the institution. Therefore, contracts and service level agreements should include a clear definition of roles and responsibilities, misuse of electronic personal information and the penalties that may be imposed in the event of a breach of contract or lack of service as per the defined service levels in relation to electronic personal information. A breach of contract may be the lack of security safeguards by the third party resulting in a data breach of electronic personal information and a lack of service may be the inability of a third party to provide access to electronic personal information.

Lastly, the *M5: Business Continuity Management* security safeguard ensures that the recovery of electronic personal information in the event of a business interruption should not be overlooked. As such, the processes and parameters for acceptable recovery of electronic personal information should be defined as part of the business continuity plan. In addition, the recovery of electronic personal information should also form part of the testing associated with business continuity management processes.

9.4.2 OPERATIONAL COMPONENT

The operational component of the model of operation of security safeguards is associated with 6 security safeguards, as illustrated in Figure 9.5 below, which encapsulates the execution of processes driven from a people perspective.



OPERATIONAL COMPONENT (EXECUTION OF PROCESSES - PEOPLE DRIVEN)

O1 - SECURITY PROCEDURES AND PROCESSES
CHANGE AND CONFIGURATION MANAGEMENT, AVAILABILITY MANAGEMENT, INCIDENT MANAGEMENT, BACKUP MANAGEMENT, USER ACCOUNT AND ACCESS MANAGEMENT AND KEY MANAGEMENT PROCEDURES AND PROCESSES

O2 - BASELINE INFRASTRUCTURE SECURITY STANDARDS
SERVER, WORKSTATION AND LAPTOP OPERATING SYSTEMS, DATABASE, WEB SERVER, NETWORK COMPONENT (FIREWALLS, ROUTERS, WIRELESS) SECURITY STANDARDS

O3 - SECURITY AWARENESS AND TRAINING
EMPLOYEE, CONTRACTOR OR THIRD PARTY OPERATOR SECURITY AWARENESS AND TRAINING SESSIONS

O4 - SECURITY MONITORING, INCIDENT AND REPORTING
CENTRALISED AUDIT LOGGING MONITORING AND INCIDENT MANAGEMENT PROCESSES PROVIDE THE PLATFORM FOR SECURITY REPORTING TO DIFFERENT STAKEHOLDERS AS REQUIRED

O5 - SECURITY ASSESSMENT
ASSESSMENT OF THE TECHNICAL, ORGANISATIONAL, PROCEDURAL, ADMINISTRATIVE OR PHYSICAL SECURITY POSTURE

O6 - DISASTER RECOVERY
PEOPLE, PROCESSES AND TECHNOLOGY REQUIRED TO ENSURE CONTINUED OPERATIONS IN THE EVENT OF A DISASTER

Figure 9.5: Model of Operation of Security Safeguards - Operational Component

The *O1: Security Procedures and Processes* security safeguard within the operational component requires the definition, approval and implementation of security procedures and processes to address electronic personal information. As such, security procedures and processes for change and configuration management, patch management, availability management, incident management, backup management, user account and access management as well as the management of encryption keys to secure data channels and enforce encryption should be defined or updated if they already exist, to specifically make provision for electronic personal information.

To prevent the adoption of default configurations and to ensure consistent configurations of all technology infrastructure (server, workstation and laptop operating systems, database servers, network components (firewalls, routers, wireless) and web servers), which store, process or transmit electronic personal information, the *O2: Baseline Infrastructure Security Standards* security safeguard within the operational component requires the definition of baseline infrastructure security standards. Once defined, the baseline infrastructure security standards should be approved for implementation.

The *O3: Security Awareness and Training* security safeguard within operational component specifies the need for employees, contractors or third party operators to be provided with security awareness and training, specifically focused on securing electronic personal information. The security awareness and training may take the form of formal awareness and training sessions as well as via communication platforms such as posters, videos and emails.

In order for the *O4: Security Monitoring, Incident and Reporting* security safeguard within the operational component to be effective, all audit logs from applications as well as the technology infrastructure associated with electronic personal information needs to maintain audit logs. This will enable security monitoring, incident identification and reporting for all applications and the technology infrastructure associated with electronic personal information. In addition, security monitoring should encompass persistent and remote asset tracking of all information assets that store, process or transmit electronic personal information. The incident aspect of this safeguard should provide for the ability to identify a security incident associated electronic personal information. Lastly, the reporting aspect of this safeguard should cater for the ability to report on any malicious activities or data breaches of electronic personal information.

The *O5: Security Assessment* security safeguard is in place to test the security posture from a technical, institutional, procedural, administrative or physical security perspective as it relates to electronic personal information. As such, security assessments in the form of penetration tests should be performed on a regular basis to identify technical, organisational, procedural, administrative or physical security weaknesses. The weaknesses identifies should be dealt with in an effective and efficient manner to ensure the confidentiality and integrity of electronic personal information.

In the event of a disaster, to continue operations electronic personal may be required by the institution therefore the *O6: Disaster Recovery* security safeguard within the operational component requires the people, processes and technology associated with electronic personal information to be defined. As such in the event of a disaster, the people, processes and technology associated with electronic personal information should enable the recovery of the required electronic personal information to ensure continued operations.

The security procedures and processes, baseline infrastructure security standards, security awareness and training, security monitoring, incident and reporting as well as the security assessment security safeguards within the operational component are as a result of the information security policy and risk management security safeguards of the management component. In addition, the security monitoring, incident and reporting security safeguard of the operational component is utilised to enforce the supplier and service level management aspect within the management domain. The disaster recovery security safeguard of the operational component provides the people, processes and technology required to ensure continued operations in the event of a disaster and is a direct result of the business continuity management security safeguard of the management component.

9.4.3 TECHNICAL COMPONENT

The technical component of the model of operation of security safeguards is associated with 9 security safeguards, as illustrated in Figure 9.6 below, is technology driven to enable the execution of security safeguards.

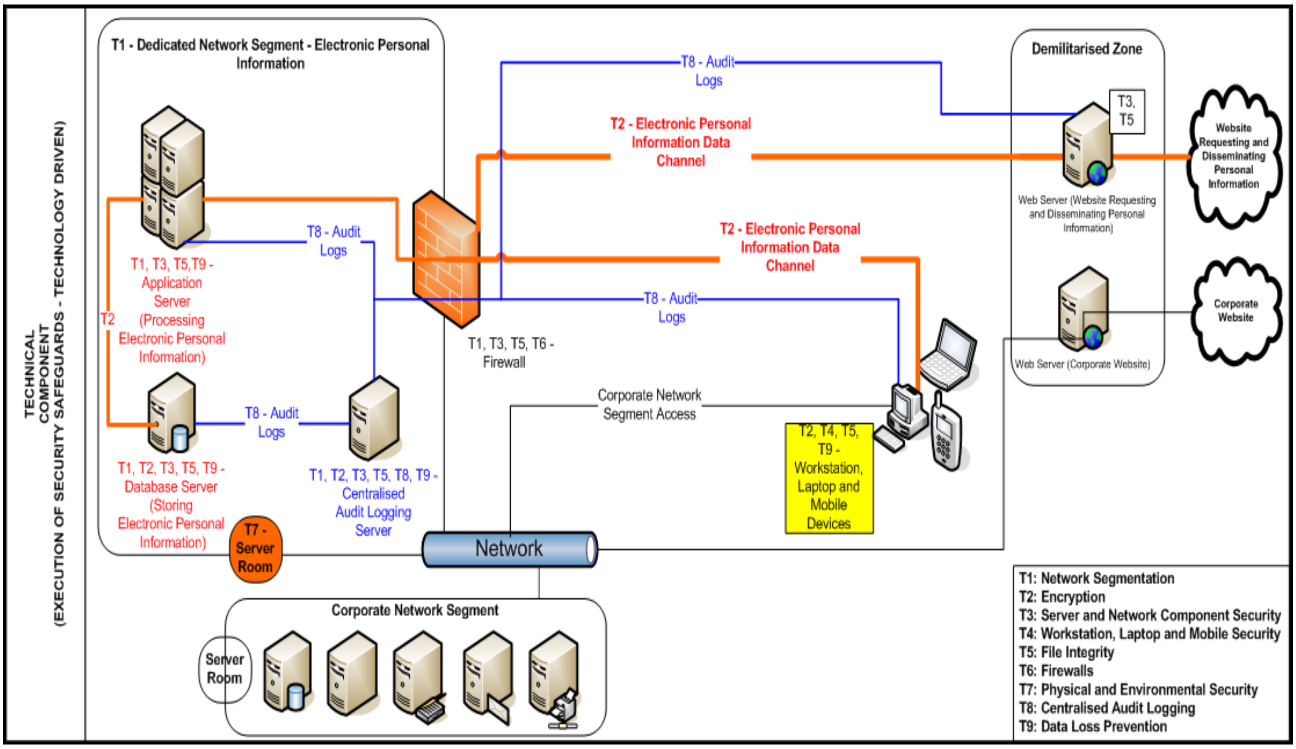

TECHNICAL COMPONENT
(EXECUTION OF SECURITY SAFEGUARDS - TECHNOLOGY DRIVEN)
T1 - Dedicated Network Segment - Electronic Personal Information
T1, T3, T5,T9 - Application Server (Processing Electronic Personal Information)
T2
T8 - Audit Logs
T1, T2, T3, T5, T9 - Database Server (Storing Electronic Personal Information)
T8 - Audit Logs
T1, T2, T3, T5, T8, T9 - Centralised Audit Logging Server
T7 - Server Room
T8 - Audit Logs
T2 - Electronic Personal Information Data Channel
T2 - Electronic Personal Information Data Channel
T8 - Audit Logs
T1, T3, T5, T6 - Firewall
Corporate Network Segment Access
T2, T4, T5, T9 - Workstation, Laptop and Mobile Devices
Network
Corporate Network Segment
Server Room
Demilitarised Zone
T3, T5
Web Server (Website Requesting and Disseminating Personal Information)
Website Requesting and Disseminating Personal Information
Web Server (Corporate Website)
Corporate Website
T1: Network Segmentation
T2: Encryption
T3: Server and Network Component Security
T4: Workstation, Laptop and Mobile Security
T5: File Integrity
T6: Firewalls
T7: Physical and Environmental Security
T8: Centralised Audit Logging
T9: Data Loss Prevention

Figure 9.6: Model of Operation of Security Safeguards - Technical Component

The model of operation of security safeguards is premised on the centralisation of electronic personal information and this is supported by the *T1: Network Segmentation* security safeguard. As such, the *T1: Network Segmentation* security safeguard will enable the creation of a central point for the processing and storing of electronic personal information. Therefore, all application and database servers that respectively process and store electronic personal information should be located on a dedicated network segment (may be a wired or wireless network or a combination thereof) that is separated from the rest of the corporate network.

The *T2: Encryption* safeguard is the next security safeguard within the technical component of the model of operation of safeguards. This safeguard deals with the encryption of all electronic personal information that is stored or transmitted. Therefore, all information assets, such as databases, which store electronic personal information should be identified and encrypted. In addition, all electronic personal information transmitted (flowing into and out of the dedicated network segment) should take place over encrypted data channels, therefore it is critical to identify all data channels associated with electronic personal information flowing into and out of the dedicated network segment. The use of encryption will significantly increase the ability to preserve the confidentiality and integrity of electronic personal information.

The next security safeguard *T3: Server and Network Component Security* deals with implementing the approved baseline infrastructure security standards defined within the *O2: Baseline Infrastructure Security Standards* security safeguard as part of the operational component of the model of operation of security safeguards. As such, all technology infrastructure components (server, workstation and laptop operating systems, database servers, network (firewalls, routers, wireless) and web servers), which store, process or transmit electronic personal information should be configured in accordance with the approved baseline infrastructure standards.

The security safeguard *T4: Workstation, Laptop and Mobile Security* is applicable to workstations, laptops and mobile devices in a similar fashion to the security safeguard *T3: Server and Network Component Security*, which was applicable to server and network components. As such, all workstations, laptops and mobile devices in an institution, with access to electronic personal information should be configured in accordance with the approved baseline infrastructure standards. Furthermore, workstations and laptops should be locked down to prevent users to change the configuration or install additional applications. In addition, to track the location of workstations, laptops and mobile devices, if supported, firmware basic input output system (BIOS) based tracking should be implemented.

The *T5: File Integrity* security safeguard ensures the integrity of all configurations associated with server and network components. Therefore, after configuring all server and network components which store, process or transmit electronic personal information in accordance with the approved baseline infrastructure standards, each configuration should be associated with a unique value known as a hash value. Thereafter, on a regular basis, to ensure that no unauthorised changes were affected to configurations of server and network devices hash value validation should be performed. This validation entails comparing the hash value associated with configuration to the hash value generated during hash value validation, if no changes were affected to the configuration the hash values should match and in the event of unauthorised changes to the configuration the hash values will not match. In the event of authorised changes to a configuration as a result of an approved update to the baseline infrastructure standard, a new hash value should be generated to be associated with the updated configuration.

The next security safeguard *T6: Firewalls* enables the separation of the application and database servers that respectively process and store electronic personal information located on a dedicated network segment from the rest of the corporate network. Therefore, a firewall should be deployed as part of the dedicated network segment to create the segmentation between the dedicated network segment and the corporate network segment. In addition, the firewall should be used to control access to the dedicated network segment.

In terms of the security safeguard, *T7: Physical and Environmental Security*, physical and environmental security safeguards need to be in place within the server rooms hosting the applications as well as the technology infrastructure associated with the storage, processing and transmission of electronic personal information. Physical security safeguards will allow for physically securing the server rooms hosting the applications as well as the technology infrastructure associated electronic personal information by strictly controlling physical access to the server rooms. To address environmental hazards such as floods and fire the server rooms require environmental controls to be deployed to mitigate the associated risk.

The *T8: Centralised Audit Logging* security safeguard necessitates audit logs to be maintained for all applications as well as the technology infrastructure associated with storing, processing and transmitting electronic personal information. These audit logs should be sent to a centralised audit logging server located in the dedicated network segment. The centralised audit logging server should analyse the audit logs in order to identify ineffective security safeguards and security incidents. In addition, the centralised audit logging based on the audit logs maintained will play a critical part when conducting an investigation in the event of a data breach of electronic personal information.

Lastly the *T9: Data Loss Prevention* security safeguard enables the prevention of electronic personal information within the institution specifically focused on workstations, laptops and mobile devices. As such, data loss prevention should be enforced on workstations, laptops or mobile devices that have access to electronic personal information. In addition, as an additional layer of security it is also recommended to implement data loss prevention on servers within the dedicated network segment such as the application, database and centralised audit logging servers to prevent the loss of electronic personal information.

Based on how the security safeguards within the technical component of the model of operation of safeguards should be implemented, Table 9.4 below demonstrates the relationship between the information assets, data channels and the associated security safeguards within the technical component of the model of operation of safeguards as illustrated in Figure 9.6 above. The process to identify the information assets is provided and illustrated in Table 9.2 above within section 9.3 of this chapter.

Table 9.4: Relationship between the Information Assets, Data Channels and the Associated Security Safeguards

Information asset / data channel	**Associated security safeguard (technical component)**
Dedicated Network Segment	*T1: Network Segmentation* - The dedicated network segment that is created which is separated from the corporate network

Information asset / data channel	**Associated security safeguard (technical component)**
	segment and consists of the application server (processing electronic personal information), database server (storing electronic personal information) and the centralised audit logging server.
Application Server (Processing Electronic Personal Information)	*T1: Network Segmentation* - The application server processing electronic personal information forms part of the dedicated network segment. *T3: Server and Network Component Security* - The application server processing electronic personal information is configured in accordance with the approved baseline infrastructure security standards. *T5: File Integrity* - The configuration of the application server processing electronic personal information is associated with a hash value and via file integrity monitoring it is subject to hash value validation to ensure no unauthorised changes to the configuration implemented as per the approved baseline infrastructure security standards. *T9: Data Loss Prevention* - The application server processing electronic personal information implements data loss prevention to prevent the loss of electronic personal information.
Database Server (Storing Electronic Personal Information)	*T1: Network Segmentation* - The database server storing electronic personal information forms part of the dedicated network segment. *T2: Encryption* - The database server storing electronic

Information asset / data channel	**Associated security safeguard (technical component)**
	personal information is encrypted. *T3: Server and Network Component Security* - The database server storing electronic personal information is configured in accordance with the approved baseline infrastructure security standards. *T5: File Integrity* - The configuration of the database server storing electronic personal information is associated with a hash value and via file integrity monitoring it is subject to hash value validation to ensure no unauthorised changes to the configuration implemented as per the approved baseline infrastructure security standards. *T9: Data Loss Prevention* - The database server storing electronic personal information implements data loss prevention to prevent the loss of electronic personal information.
Centralised Audit Logging Server	*T1: Network Segmentation* - The centralised audit logging server forms part of the dedicated network segment. *T2: Encryption* - The centralised audit logging server is encrypted to secure the audit logs stored for further analysis. *T3: Server and Network Component Security* - The centralised audit logging server is configured in accordance with the approved baseline infrastructure security standards. *T5: File Integrity* - The configuration of the centralised audit

Information asset / data channel	**Associated security safeguard (technical component)**
	logging server is associated with a hash value and via file integrity monitoring it is subject to hash value validation to ensure no unauthorised changes to the configuration implemented as per the approved baseline infrastructure security standards. *T8: Centralised Audit Logging* - All audit logs from workstations, laptops, mobile devices, the web site requesting and disseminating electronic personal information as well as the audit logs from the application server processing electronic personal information and the database server storing electronic personal information is sent for analysis to the centralised audit logging server. *T9: Data Loss Prevention* - The centralised audit logging server implements data loss prevention to prevent the loss of audit logs stored for further analysis.
Server Room	*T7: Physical and Environmental Security* - The server room hosting the applications as well as the technology infrastructure (dedicated network segment which contains the application, database and centralised audit logging servers) associated with the storage, processing and transmission of electronic personal information implements physical and environmental security.
Firewall	*T3: Server and Network Component Security* - The firewall is configured in accordance with the approved baseline infrastructure security standards. *T5: File Integrity* - The configuration of the firewall is associated

Information asset / data channel	Associated security safeguard (technical component)
	with a hash value and via file integrity monitoring it is subject to hash value validation to ensure no unauthorised changes to the configuration implemented as per the approved baseline infrastructure security standards. *T6: Firewalls* - The firewall is implemented to control access to the dedicated network segment that hosts the application, database and centralised audit logging servers.
Workstations, Laptops or Mobile Devices	*T2: Encryption* - The workstations, laptops or mobile devices are encrypted to secure the associated electronic personal information. *T4: Workstation, Laptop and Mobile Security* - Workstations, laptops or mobile devices are configured in accordance with the approved baseline infrastructure security standards and locked down to prevent the user to change the configuration or install additional applications. Furthermore, firmware basic input output system (BIOS) based tracking is implemented on supported devices. *T5: File Integrity* - The configuration of workstations, laptops or mobile devices are associated with a hash value and via file integrity monitoring it is subject to hash value validation to ensure no unauthorised changes to the configuration implemented as per the approved baseline infrastructure security standards. *T9: Data Loss Prevention* - The workstations, laptops or mobile devices implement data loss prevention to prevent the loss of electronic personal information and asset tracking is enabled

Information asset / data channel	**Associated security safeguard (technical component)**
	on workstations, laptops or mobile devices that do not support firmware basic input output system (BIOS) based tracking.
Web Server (Web site Requesting and Disseminating Electronic Personal Information)	*T3: Server and Network Component Security* - The web server hosting the web site requesting and disseminating electronic personal information is configured in accordance with the approved baseline infrastructure security standards. *T5: File Integrity* - The configuration of the web server hosting the web site requesting and disseminating electronic personal information is associated with a hash value and via file integrity monitoring it is subject to hash value validation to ensure no unauthorised changes to the configuration implemented as per the approved baseline infrastructure security standards.
Electronic Personal Information Data Channel	*T2: Encryption* - All data channels that enable the transmission of electronic personal information are encrypted.

In essence, the security safeguards within the technical component of the model of operation of safeguards, as illustrated in Figure 9.6, involves segmenting the network to include application, database and other servers associated with electronic personal information in a separate dedicated network segment from the rest of the corporate network. Furthermore, all electronic personal information that enters or leaves the separate dedicated network segment should utilise encrypted data channels as well as a firewall at the perimeter of the dedicated network segment. The servers, network components, workstations and laptops that store, process and transmit personal information should be secured by the implementation of the defined and approved baseline infrastructure security standards. These configurations should form part of file integrity monitoring processes via hash value validation to identify any changes to the configurations. Physical access to the server rooms where the actual servers are located that store, process and transmit electronic personal information should be strictly controlled and the server room should appropriately mitigate risks associated with environmental hazards. In the event of a data breach where electronic personal information is compromised a central audit logging server which should maintain audit logs of all applications and technology infrastructure components will serve as the critical evidence source during an investigation. Lastly, data loss prevention should be implemented to ensure that electronic personal information is not leaked from workstations, laptops or mobile devices as well as servers that store, process and transmit electronic personal information.

The model of operation of security safeguards through the management, operational and technical components clearly guides one on how the selection of security safeguards as per section 9.2 of this chapter should be implemented to achieve and maintain confidentiality and integrity of electronic personal information as required by Condition 7 of the POPI Act (2013). The next section which follows provides a critical evaluation of the model of operation of security safeguards.

9.5 Critical Evaluation - Benefits and Limitations

A critical evaluation of the model of operation of security safeguards led to the identification of benefits and limitations associated with the model of operation of security safeguards.

Sikhungo (2016) states that: “POPI does not provide a “tick list” of security requirements to meet”. Gawande (2012) is however a huge proponent of the “tick list” approach, also referred to as the “checklist” approach, and argues that it is often overlooked when addressing complex problems and provides a means to ensure that all aspects are covered quickly and concisely. As such a major benefit of the model of operation of security safeguards is that it not only provides South African institutions with a “tick list” of security requirements in the form of the selection of security safeguards within the proposed POPI Condition 7 framework (which were validated by 167 participants), but goes a step further by providing guidance on how the selection of security safeguards within the proposed POPI Condition 7 framework should be implemented to achieve and maintain confidentiality and integrity of electronic personal information as required by Condition 7 of the POPI Act (2013).

The model of operation of security safeguards may be applied within any institution in the public or private sector, independent of the institution size or industry sector, that needs to ensure confidentiality and integrity of electronic personal information required to ultimately achieve and maintain compliance with Condition 7 of the POPI Act (2013).

Furthermore, the model of operation of security safeguards has a pre-requisite for identifying all electronic personal information stored, processed or transmitted by an institution. As a result, an approach to identify all the electronic personal information is provided as part of the model of operation of security safeguards as a precursor in section 9.3 of Chapter 9.

Another major benefit associated with the model of operation of security safeguards is that from a technical component perspective, since the model of operation of security safeguards is premised on the creation of a dedicated network segment for the processing and storing of electronic personal information, separate from the corporate network, it may be applied to centralised or decentralised architectures. In a centralised architecture a single dedicated network segment is created and the storage and processing of electronic personal information all occurs at the single dedicated network segment. For example, in a centralised architecture if the single dedicated network segment is at head office and when electronic personal information is received at a regional level, this information will be transmitted to the single dedicated network segment at head office for storage or processing. An advantage of applying the model of operation of safeguards to a centralised architecture is that it offers easier administration, reduces the need to apply multiple safeguards in multiple locations.

In a decentralised architecture there is more than one dedicated network segment for the processing and storing of electronic personal information. For example, in a decentralised architecture there is a dedicated network segment at head office for all storage and processing of electronic personal information in that environment and there are dedicated network segments at regional level for storing and processing electronic personal information at those specific levels. An advantage of applying the model of operation of safeguards to a decentralised architecture is that it eliminates a central point of failure and offers enhanced performance with multiple locations for storing and processing electronic personal information.

In addition, the model of operation of security safeguards applies the defence in depth principle (several security safeguards in place instead of a single security safeguard to protect information assets) based on the selection of security safeguards from the proposed POPI Condition 7 framework associated with the model of operation of security safeguards. For example, the dedicated network segment responsible for storing and processing of electronic personal information advocates the use of a firewall (*T6: Firewalls* security safeguard) in conjunction with encrypting (*T2: Encryption* security safeguard) electronic personal information transmitted and stored.

The strategic and operational components of the model of operation of security safeguards may be applied to personal information in both electronic format (within information systems and their corresponding databases) and non-electronic format (hard copy or paper based outside information systems).

The model of operation of security safeguards is dependent on a selection of security safeguards, ideally the selection of security safeguards from the proposed POPI Condition 7 framework, in support of the management, operational and technical components defined within the model.

There are limitations associated with the application of the model of operation based on the architecture. As such, applying the model of operation of security safeguards to a centralised architecture is that it creates a central point of failure and if there are multiple locations, which are geographically dispersed there may be performance related issues impacting the processing and storage of electronic personal information. The application of the model of operation of security safeguards in a decentralised architecture may lead to greater costs as multiple security safeguards need to be implemented in multiple locations and there is a greater deal of administration required.

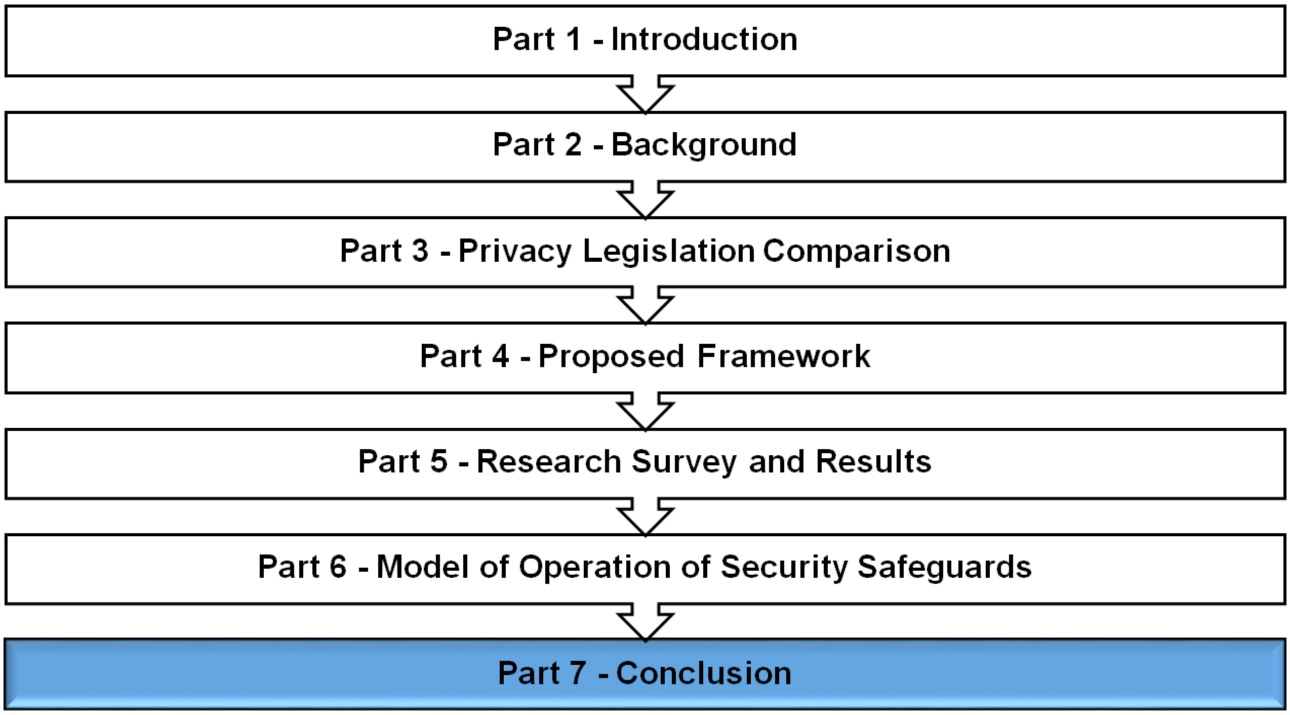
The last limitation associated with the model of operation of security safeguards is that the technical domain is applicable only to personal information in electronic format.

9.6 CONCLUSION

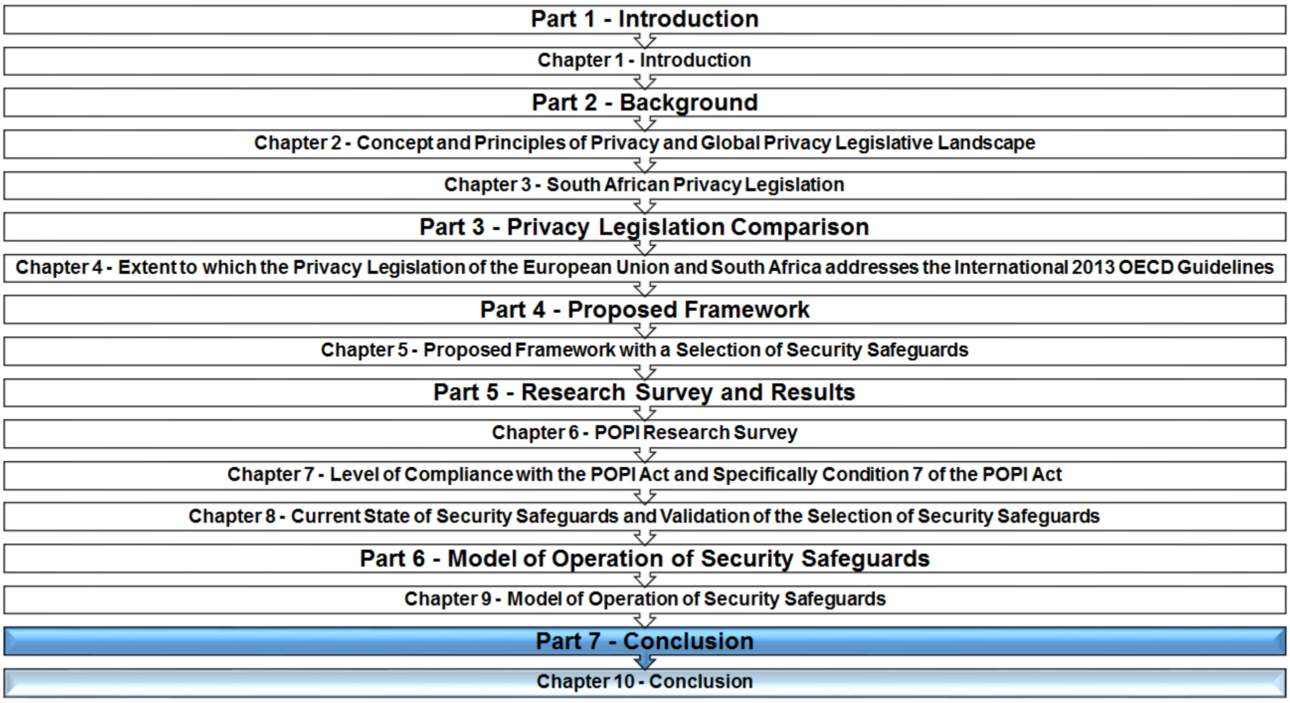
This chapter concluded Part 6 (Model of Operation of Security Safeguards) of this thesis by addressing research question 6 through a proposed model of operation of security safeguards. The proposed model of operation of security safeguards provided guidance on how the selection of security safeguards within the “Secure” phase of the proposed POPI Condition 7 framework should be implemented to achieve and maintain the confidentiality and integrity of electronic personal information as required by Condition 7 of the POPI Act (2013). This included an overview of the revised selection of security safeguards as a result of the POPI research survey results in Chapter 8 and the prerequisites applicable to the model of operation of security safeguards. Lastly, the benefits and limitations associated with the model of operation of security safeguards was provided as part of a critical evaluation.

Part 7 (Conclusion), through the final chapter which follows, is devoted to concluding this thesis.

PART 7 - CONCLUSION


Part 1 - Introduction
Part 2 - Background
Part 3 - Privacy Legislation Comparison
Part 4 - Proposed Framework
Part 5 - Research Survey and Results
Part 6 - Model of Operation of Security Safeguards
Part 7 - Conclusion

CHAPTER 10 - CONCLUSION



Part 1 - Introduction

Chapter 1 - Introduction

Part 2 - Background

Chapter 2 - Concept and Principles of Privacy and Global Privacy Legislative Landscape

Chapter 3 - South African Privacy Legislation

Part 3 - Privacy Legislation Comparison

Chapter 4 - Extent to which the Privacy Legislation of the European Union and South Africa addresses the International 2013 OECD Guidelines

Part 4 - Proposed Framework

Chapter 5 - Proposed Framework with a Selection of Security Safeguards

Part 5 - Research Survey and Results

Chapter 6 - POPI Research Survey

Chapter 7 - Level of Compliance with the POPI Act and Specifically Condition 7 of the POPI Act

Chapter 8 - Current State of Security Safeguards and Validation of the Selection of Security Safeguards

Part 6 - Model of Operation of Security Safeguards

Chapter 9 - Model of Operation of Security Safeguards

Part 7 - Conclusion

Chapter 10 - Conclusion

10.1 INTRODUCTION

In Chapter 9, a model of operation of security safeguards to guide one on how the selection of security safeguards should be implemented to achieve and maintain the confidentiality and integrity of electronic personal information as required by Condition 7 of the Protection of Personal Information (POPI) Act (Act 4 of 2013) was proposed. This chapter assesses the extent to which the research problem guided by research questions and the research objectives defined in Chapter 1 have been addressed. Furthermore, the research contribution associated with this thesis is provided followed by potential areas of future research.

10.2 RESEARCH PROBLEM ADDRESSED

Condition 7 of the POPI Act (2013), requires a selection of security safeguards to ensure the confidentiality and integrity of personal information. However, the research problem identified was that the legislative requirement of Condition 7 of the POPI Act (2013) is spelt out in Sections 19, 20, 21 and 22, but the requirements are not supported by specific guidance in terms of how the requirements should be satisfied. There is also no specific guidance on the security safeguards, as required in Section 19, to ensure the confidentiality and integrity of specifically electronic personal information for the purpose of this thesis. Sikhungo (2016) confirmed this problem and stated that: "POPI does not provide a "tick list" of security requirements to meet. Responsible parties must consider applicable industry security practices and then implement security appropriate security measures for the business." Therefore, in providing a solution to the aforementioned research problem, specifically focused on Condition 7 of the POPI Act (2013) and limited to electronic personal information, the following 6 research questions formulated and associated with the research problem were addressed as follows:

- Research question 1 - *To what extent does the privacy legislation of the European Union (EU) and South Africa addresses the international 2013 Organisation for Economic Co-operation and Development (OECD) guidelines?*

  Chapter 4 of the thesis provided an analysis in terms of the extent to which the privacy legislation of the EU and South Africa address the international 2013

Organisation for OECD guidelines. In addition, a critical evaluation of the analysis in terms of the extent to which the privacy legislation of the EU and South Africa addresses the international 2013 OECD guidelines led to the identification of similarities and differences associated with the privacy legislation compared as part of the analysis.

- Research question 2 - *How can South African institutions, who store, process and transmit electronic personal information achieve and maintain compliance with Condition 7 of the POPI Act (2013), including the security safeguards to be considered to ensure confidentiality and integrity of electronic personal information?*

  By addressing this research question a solution directly associated with the research problem was provided within Chapter 5, in the form of a proposed POPI Condition 7 framework to ultimately address the requirements of Condition 7 of the POPI Act (2013), specifically in relation to electronic personal information. The proposed POPI Condition 7 framework consisted of a 4-phased (“Identify”, “Secure”, “Monitor and Report” and “Remediate”) approach, which encapsulated a specific selection of 20 security safeguards across 3 domains (management, operational and technical) as part of the “Secure” phase to ensure confidentiality and integrity of electronic personal information stored, processed or transmitted. Furthermore, as a result of a critical evaluation, benefits and limitations associated with the POPI Condition 7 framework were identified.

- Research question 3 - *What is the current level of compliance by South African institutions to the POPI Act (2013) and specifically Condition 7 of the POPI (2013) Act?*

  Based on the analysis of the POPI research survey results associated with 167 participants the current level of compliance with the POPI Act (2013) as well as with Condition 7 of the Act was ascertained within Chapter 7. Furthermore, the analysis of the POPI research survey results provided the overall level of understanding of the POPI Act (2013) by the 167 participants who participated in the POPI research survey. In addition, the POPI research survey results provided the financial value associated with electronic personal information as well as the potential impact of a data breach of electronic personal information. Lastly, a critical evaluation led to the identification of key findings and recommendations based on the analysis of the POPI research survey results.

- Research question 4 - *What is the current state of security safeguards within South African institutions to achieve compliance with Condition 7 of the POPI Act (2013), specifically in relation to electronic personal information?*

  The analysis of the POPI research survey results associated with 167 participants provided the current state of security safeguards within South African institutions to achieve compliance with Condition 7 of the POPI Act (2013), specifically in relation to electronic personal information, within Chapter 8. This assessment explored the applicability, extent of implementation and completeness of the selection of security safeguards proposed as part of the “Secure” of the proposed POPI Condition 7 framework. In addition, a critical evaluation led to the identification of key findings and recommendations based on the analysis of the POPI research survey results.

- Research question 5 - *To what extent is the selection of security safeguards proposed as part of the framework within this thesis valid?*

  By obtaining an understanding the current state of security safeguards in terms of applicability and completeness, the validity of the selection of security safeguards within the proposed POPI Condition 7 framework was provided in Chapter 8 of this thesis. Furthermore, as a result of the outcome of the validity of the selection of security safeguards within the proposed POPI Condition 7 framework, key findings and recommendations were identified as part of a critical evaluation.

- Research question 6 - *How can the security safeguards proposed as part of the framework within this thesis be implemented to achieve and maintain confidentiality and integrity of electronic personal information as required by Condition 7 of the POPI Act (2013)?*

  A model of operation of security safeguards was proposed in Chapter 9 to guide one on how the selection of security safeguards within the “Secure” phase of the proposed POPI Condition 7 framework should be implemented to achieve and maintain confidentiality and integrity of electronic personal information as required by Condition 7 of the POPI Act (2013). Furthermore, as a result of a critical evaluation benefits and limitations associated with the model of operation of security safeguards were identified.

10.3 Research Objectives Accomplished

Taking into account the research goal and scope in conjunction with the research problem and associated research questions, this thesis accomplished the following research objectives:

- Explored the concept and principles of privacy as well as the importance of privacy. It also provided an overview of the global privacy legislative landscape within Chapter 2.
- Provided an overview of South African privacy legislation in Chapter 3.
- Analysed, in Chapter 4, the extent to which the privacy legislation of the EU and South Africa addresses the international 2013 OECD guidelines.
- Chapter 5 proposed a framework that includes a selection of security safeguards that may serve as a frame of reference and be used by South African institutions that store, process and transmit electronic personal information, to ultimately achieve and maintain compliance with Condition 7 of the POPI Act (2013).
- Assessed the level of compliance with the POPI Act (2013) and specifically Condition 7 of the Act through the POPI research survey aimed at participants from South African institutions within Chapter 7.

- Chapter 8 assessed, through the POPI research survey aimed at participants from South African institutions, the current state of security safeguards within South African institutions to achieve compliance with Condition 7 of the POPI Act (2013), specifically related to electronic personal information.
- Validated the selection of security safeguards of the proposed POPI Condition 7 framework, as part of Chapter 8, by evaluating the applicability and completeness of the selection of security safeguards through the POPI research survey aimed at participants from South African institutions who store, process and transmit electronic personal information.
- Chapter 9 proposed a model of operation of security safeguards to guide how the selection of security safeguards should be implemented to achieve and maintain the confidentiality and integrity of electronic personal information as required by Condition 7 of the POPI Act (2013).

10.4 RESEARCH CONTRIBUTION

In light of the achievement of the research objectives there are 2 major research contributions made by this thesis. Firstly, the proposed POPI Condition 7 framework within Chapter 5 would now provide South African institutions with a 4-phased approach to ultimately address the requirements of Condition 7 of the POPI Act (2013), specifically in relation to electronic personal information. In addition, the “Secure” phase of the proposed POPI Condition 7 framework provides specific guidance on the security safeguards, as required in Section 19, to ensure the confidentiality and integrity of specifically electronic personal information. The second major research contribution associated with this thesis is the model of operation of security safeguards as it would provide South African institutions with guidance on how the selection of security safeguards should be implemented to achieve and maintain the confidentiality and integrity of electronic personal information as required by Condition 7 of the POPI Act (2013). In essence, the proposed POPI Condition 7 framework and model of operation of safeguards will greatly assist South African institutions in their journey to achieve and maintain compliance with Condition 7 of the POPI Act (2013) by ensuring the confidentiality and integrity of electronic personal information stored, processed or transmitted.

Furthermore, this thesis may be associated with a research contribution in terms of the concept and principles of privacy, importance of privacy, global privacy legislative landscape and an overview of the South African privacy legislation. This is followed by the research contribution based on the analysis in terms of the extent to which the privacy legislation of the EU and South Africa address the international 2013 OECD guidelines. Lastly, a research contribution is made as it relates to the assessment of the level of compliance with the POPI Act (2013) and specifically Condition 7 of the Act, as well as the current state of security safeguards within South African institutions to achieve compliance with Condition 7 of the POPI Act (2013), specifically related to electronic personal information.

10.5 Future Research

Future research may be conducted in 3 areas as a result of this thesis. Firstly, an analysis in terms of the extent to which revised privacy legislation of the EU effective from 25 May 2018 addresses the international 2013 OECD guidelines. Secondly, an assessment of the level of compliance with the POPI Act (2013) and specifically Condition 7 of the Act as well as the state of security safeguards within South African institutions after the grace period of 1 year to comply expires upon the enforcement of the POPI Act (2013), which is still to be announced. Lastly, upon the enforcement of the POPI Act (2013), an analysis of the extent to which the proposed POPI Condition 7 framework and model of operation of safeguards assisted South African institutions in their journey to achieve and maintain compliance with Condition 7 of the POPI Act (2013) by ensuring the confidentiality and integrity of electronic personal information stored, processed or transmitted.

Furthermore, in order for the proposed POPI Condition 7 framework and model of operation of safeguards to transcend the academic sphere and reach South African institutions to ultimately assist them in their journey to achieve and maintain compliance with Condition 7 of the POPI Act (2013), by ensuring the confidentiality and integrity of electronic personal information stored, processed or transmitted, this thesis will be made available in the University of Pretoria library and further promoted on social media platforms. In addition, a meeting will be scheduled with the Information Regulator (POPI

Act, 2013) to share the proposed POPI Condition 7 framework and the model of operation of safeguards as this may serve as a frame of reference and assist the Information Regulator when developing further regulations, guidelines or practice notes in support of the POPI Act (2013).

10.6 CONCLUSION

Part 7 (Conclusion) of this thesis in this chapter served to conclude the research and as such assessed the extent to which the research problem, guided by research questions and research objectives defined in Chapter 1, were addressed. This was followed by the research contribution associated with the thesis as well as the potential areas of future research.

This chapter is followed by the appendices associated with this thesis as well as a bibliography of research consulted during the formulation of this thesis.

APPENDICES

APPENDIX A - SUMMARY OF HIGH PROFILE DATA BREACHES

Institution	Data breach details
Ashley Madison	37 million records exposed including names, hashed passwords, addresses, phone numbers and transaction information.
Korean Pharmaceutical Information Centre	Medical information exposed relating to approximately 90% of the South Korean population.
Sony Entertainment	Emails between Sony executives, copies of unreleased movies, salaries of executives and movie stars, and personal information, including social security numbers of employees and their dependents exposed.
U.S. Office of Personnel Management	21.5 million past, present and potential employee records exposed, which included social security numbers, names, addresses, and for some employee records detailed financial and personal information needed to obtain a security clearance, including fingerprints.
Target	40 million customer credit and debit card records exposed.
AdultFriendFinder.com	Personal information associated with 412 million users exposed.
Cisco	Personal information of job-seekers exposed.
Dropbox	68 million user email addresses and passwords exposed.
Internal Revenue Service (IRS)	Personal information associated with 700 000 American taxpayers exposed.
LinkedIn	117 million user email addresses and passwords exposed.
Philippine Commission on Elections	Personal information of every single voter in the Philippines exposed, equating to approximately 55 million people.
Snapchat	Personal information associated with 700 current and former employees exposed.
Yahoo	Personal information associated with 1 billion Yahoo accounts exposed.

Source: Adapted from Identity Force (2016) and Internet Society (2016)

APPENDIX B - MINIMUM REQUIREMENTS OF THE POPI ACT

Chapter number	Chapter description	Section
1	Definitions and purpose	1. Definitions 2. Purpose of Act
2	Applications provisions	3. Application and interpretation of Act 4. Lawful processing of personal information 5. Rights of data subjects 6. Exclusions 7. Exclusion for journalistic, literary or artistic Purposes
3	Conditions for lawful processing of personal information	
	Part A - Processing of personal information in general	
	Condition 1 - Accountability	8. Responsible party to ensure conditions for lawful processing
	Condition 2 - Processing limitation	9. Lawfulness of processing 10. Minimality 11. Consent, justification and objection 12. Collection directly from data subject
	Condition 3 - Purpose specification	13. Collection for specific purpose 14. Retention and restriction of records
	Condition 4 - Further processing limitation	15. Further processing to be compatible with purpose of collection
	Condition 5 - Information quality	16. Quality of information
	Condition 6 -	17. Documentation

Chapter number	Chapter description	Section
	Openness	18. Notification to data subject when collecting personal information
	Condition 7 - Security safeguards	19. Security measures on integrity and confidentiality of personal information 20. Information processed by operator or person acting under authority 21. Security measures regarding information processed by operator 22. Notification of security compromises
	Condition 8 - Data subject participation	23. Access to personal information 24. Correction of personal information 25. Manner of access
	Part B - Processing of special personal information	26. Prohibition on processing of special personal information 27. General authorisation concerning special personal information 28. Authorisation concerning data subject's religious or philosophical beliefs 29. Authorisation concerning data subject's race or ethnic origin 30. Authorisation concerning data subject's trade union membership 31. Authorisation concerning data subject's political persuasion 32. Authorisation concerning data subject's health or sex life 33. Authorisation concerning data subject's

Chapter number	**Chapter description**	**Section**
		criminal behaviour or biometric information
	Part C - Processing of personal information of children	34. Prohibition on processing personal information of children 35. General authorisation concerning personal information of children
4	Exemption from conditions for processing of personal information	36. General 37. Regulator may exempt processing of personal information 38. Exemption in respect of certain functions
5	Supervision	
	Part A - Information Regulator	39. Establishment of Information Regulator 40. Powers, duties and functions of Regulator 41. Appointment, term of office and removal of members of Regulator 42. Vacancies 43. Powers, duties and functions of Chairperson and other members 44. Regulator to have regard to certain matters 45. Conflict of interest 46. Remuneration, allowances, benefits and privileges of members 47. Staff 48. Powers, duties and functions of chief executive officer 49. Committees of Regulator 50. Establishment of Enforcement Committee

Chapter number	Chapter description	Section
		51. Meetings of Regulator 52. Funds 53. Protection of Regulator 54. Duty of confidentiality
	Part B - Information Officer	55. Duties and responsibilities of Information Officer 56. Designation and delegation of deputy information officers
6	Prior authorisation	57. Processing subject to prior authorisation 58. Responsible party to notify Regulator if processing is subject to prior authorisation 59. Failure to notify processing subject to prior authorisation
7	Codes of Conduct	60. Issuing of codes of conduct 61. Process for issuing codes of conduct 62. Notification, availability and commencement of code of conduct 63. Procedure for dealing with complaints 64. Amendment and revocation of codes of conduct 65. Guidelines about codes of conduct 66. Register of approved codes of conduct 67. Review of operation of approved code of conduct 68. Effect of failure to comply with code of Conduct
8	Rights of data subjects	69. Direct marketing by means of unsolicited electronic communications

Chapter number	Chapter description	Section
	regarding direct marketing by means of unsolicited electronic communications, directories and automated decision-making	70. Directories 71. Automated decision making
9	Trans-border information flows	72. Transfers of personal information outside Republic
10	Enforcement	73. Interference with protection of personal information of data subject 74. Complaints 75. Mode of complaints to Regulator 76. Action on receipt of complaint 77. Regulator may decide to take no action on complaint 78. Referral of complaint to regulatory body 79. Pre-investigation proceedings of Regulator 80. Settlement of complaints 81. Investigation proceedings of Regulator 82. Issue of warrants 83. Requirements for issuing of warrant 84. Execution of warrants 85. Matters exempt from search and seizure 86. Communication between legal adviser and client exempt 87. Objection to search and seizure

Chapter number	Chapter description	Section
		88. Return of warrants 89. Assessment 90. Information notice 91. Parties to be informed of result of assessment 92. Matters referred to Enforcement Committee 93. Functions of Enforcement Committee 94. Parties to be informed of developments during and result of investigation 95. Enforcement notice 96. Cancellation of enforcement notice 97. Right of appeal 98. Consideration of appeal 99. Civil remedies
11	Offences, penalties and administrative fines	100. Obstruction of Regulator 101. Breach of confidentiality 102. Obstruction of execution of warrant 103. Failure to comply with enforcement or information notices 104. Offences by witnesses 105. Unlawful acts by responsible party in connection with account number 106. Unlawful acts by third parties in connection with account number 107. Penalties 108. Magistrate’s Court jurisdiction to impose penalties 109. Administrative fines
12	General provisions	110. Amendment of laws 111. Fees

Chapter number	Chapter description	Section
		112. Regulations 113. Procedure for making regulations 114. Transitional arrangements 115. Short title and commencement

Source: Adapted from POPI Act (2013)

APPENDIX C - DATA PROTECTION DIRECTIVE

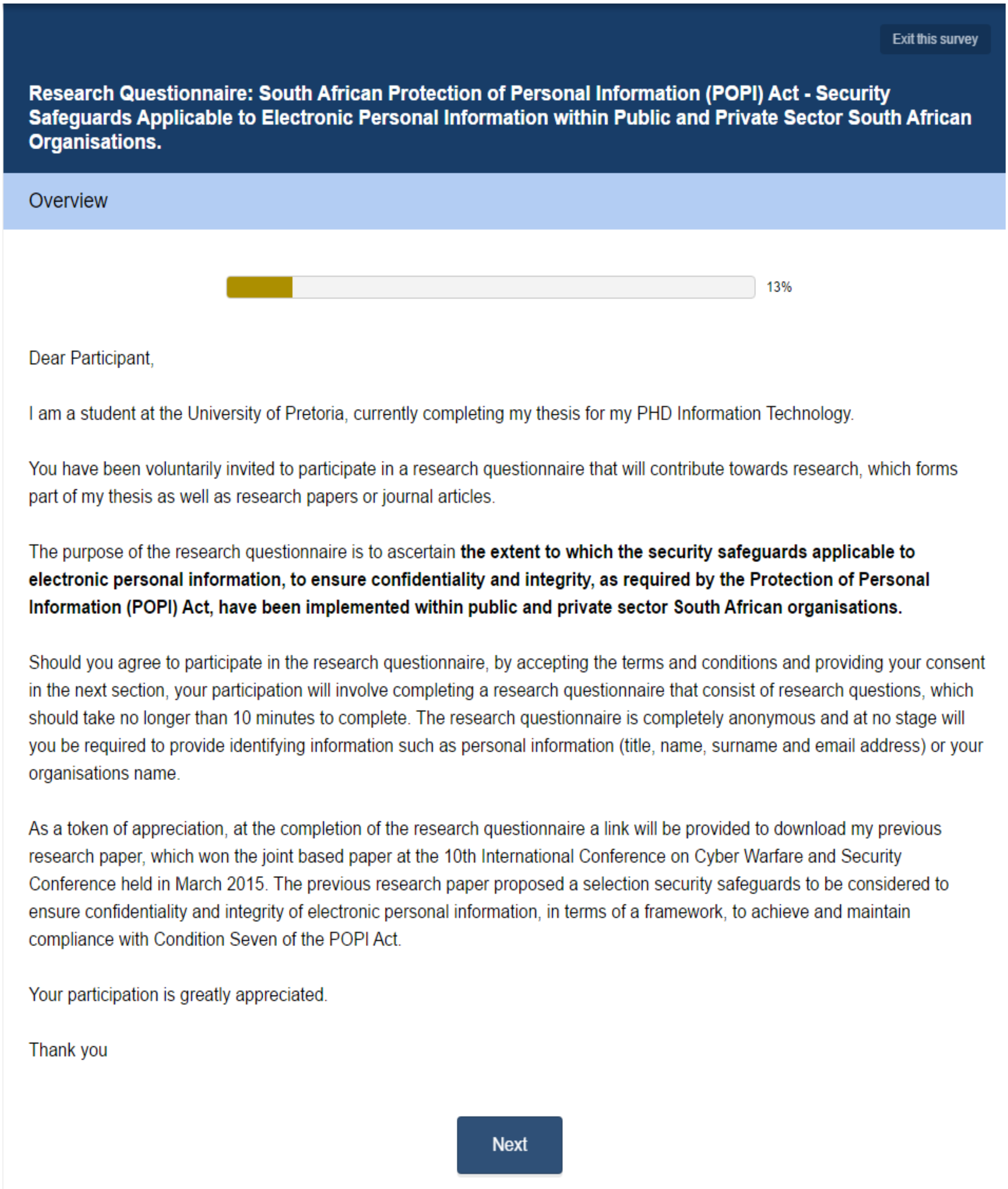
Chapter number	**Chapter title and related articles**
1	General provisions - Article 1: Object of the directive - Article 2: Definitions - Article 3: Scope - Article 4: National law applicable
2	General rules on the lawfulness of the processing of personal data - Article 5: Conditions under which the processing of personal data is lawful - Article 6: Principles relating to data quality - Article 7: Criteria for making data processing legitimate - Article 8: Processing of special categories of data - Article 9: Processing of personal data and freedom of expression - Article 10: Information in cases of collection of data from the data subject - Article 11: Information where the data have not been obtained from the data subject - Article 12: Right of access - Article 13: Exemptions and restrictions - Article 14: Data subjects right to object - Article 15: Automated individual decisions - Article 16: Confidentiality of processing - Article 17: Security of processing - Article 18: Obligation to notify the supervisory authority - Article 19: Contents of notification - Article 20: Prior checking - Article 21: Publicising of processing operations
3	Judicial remedies, liability and sanctions - Article 22: Remedies

Chapter number	**Chapter title and related articles**
	- Article 23: Liability - Article 24: Sanctions
4	Transfer of personal data to third countries - Article 25: Principles - Article 26: Derogations
5	Codes of conduct - Article 27: Codes of conduct
6	Supervisory authority and working party on the protection of individuals with regard to the processing of personal data - Article 28: Supervisory authority - Article 29 and 30: Working party on the protection of individuals with regard to the processing of personal data
7	Community implementing measures - Article 31: The committee - Article 32: Final provisions - Article 33: Commission reporting - Article 34: Directive addressed to the member states

Source: Adapted from Data Protection Directive (1995)

Appendix D - POPI Research Survey

Appendix D.1 - POPI Research Survey: Overview



Research Questionnaire: South African Protection of Personal Information (POPI) Act - Security Safeguards Applicable to Electronic Personal Information within Public and Private Sector South African Organisations.

Overview

Dear Participant,

I am a student at the University of Pretoria, currently completing my thesis for my PHD Information Technology.

You have been voluntarily invited to participate in a research questionnaire that will contribute towards research, which forms part of my thesis as well as research papers or journal articles.

The purpose of the research questionnaire is to ascertain **the extent to which the security safeguards applicable to electronic personal information, to ensure confidentiality and integrity, as required by the Protection of Personal Information (POPI) Act, have been implemented within public and private sector South African organisations.**

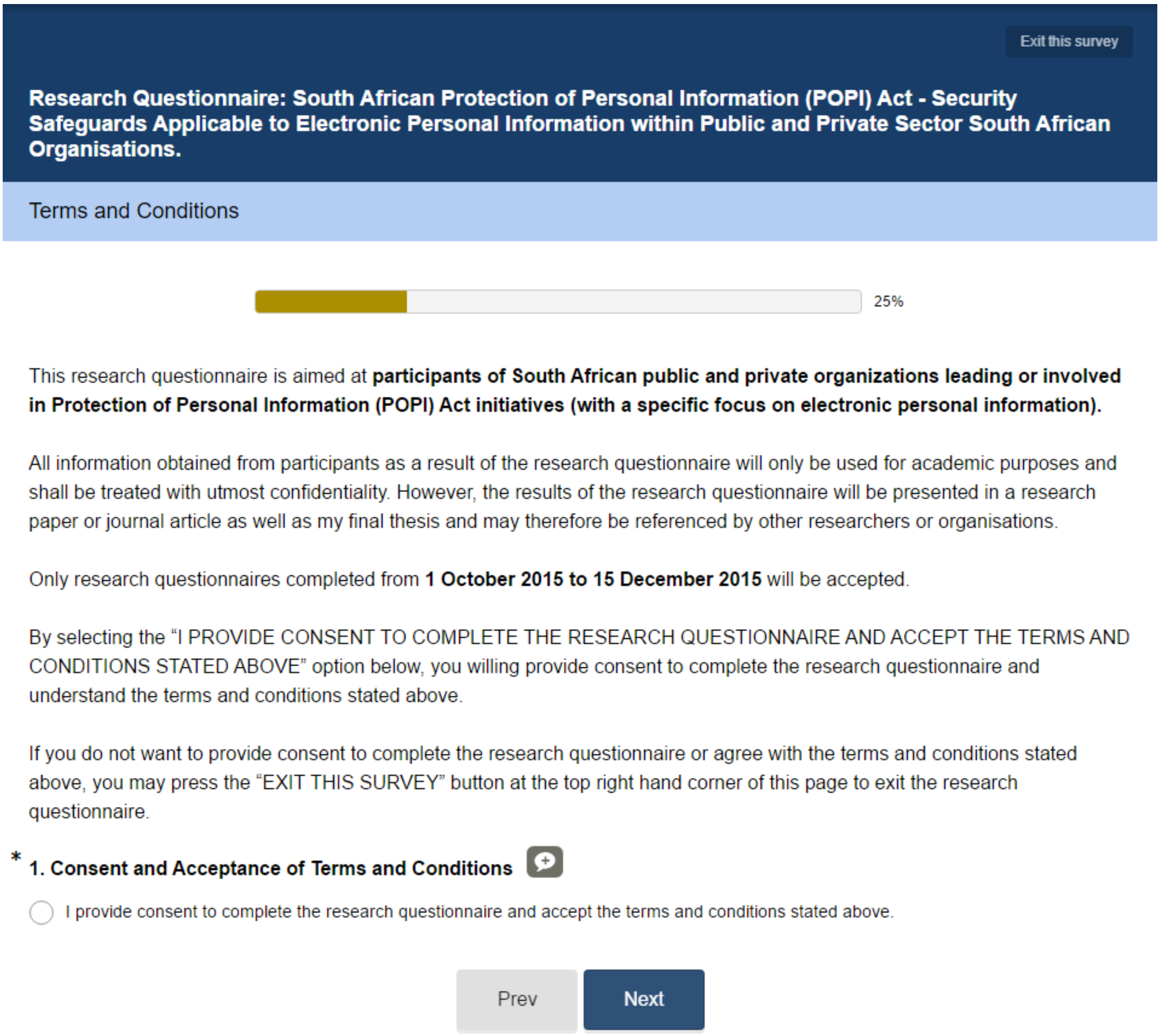
Should you agree to participate in the research questionnaire, by accepting the terms and conditions and providing your consent in the next section, your participation will involve completing a research questionnaire that consist of research questions, which should take no longer than 10 minutes to complete. The research questionnaire is completely anonymous and at no stage will you be required to provide identifying information such as personal information (title, name, surname and email address) or your organisations name.

As a token of appreciation, at the completion of the research questionnaire a link will be provided to download my previous research paper, which won the joint based paper at the 10th International Conference on Cyber Warfare and Security Conference held in March 2015. The previous research paper proposed a selection security safeguards to be considered to ensure confidentiality and integrity of electronic personal information, in terms of a framework, to achieve and maintain compliance with Condition Seven of the POPI Act.

Your participation is greatly appreciated.

Thank you

Appendix D.2 - POPI Research Survey: Terms and Conditions



Research Questionnaire: South African Protection of Personal Information (POPI) Act - Security Safeguards Applicable to Electronic Personal Information within Public and Private Sector South African Organisations.

Terms and Conditions

This research questionnaire is aimed at **participants of South African public and private organizations leading or involved in Protection of Personal Information (POPI) Act initiatives (with a specific focus on electronic personal information).**

All information obtained from participants as a result of the research questionnaire will only be used for academic purposes and shall be treated with utmost confidentiality. However, the results of the research questionnaire will be presented in a research paper or journal article as well as my final thesis and may therefore be referenced by other researchers or organisations.

Only research questionnaires completed from **1 October 2015 to 15 December 2015** will be accepted.

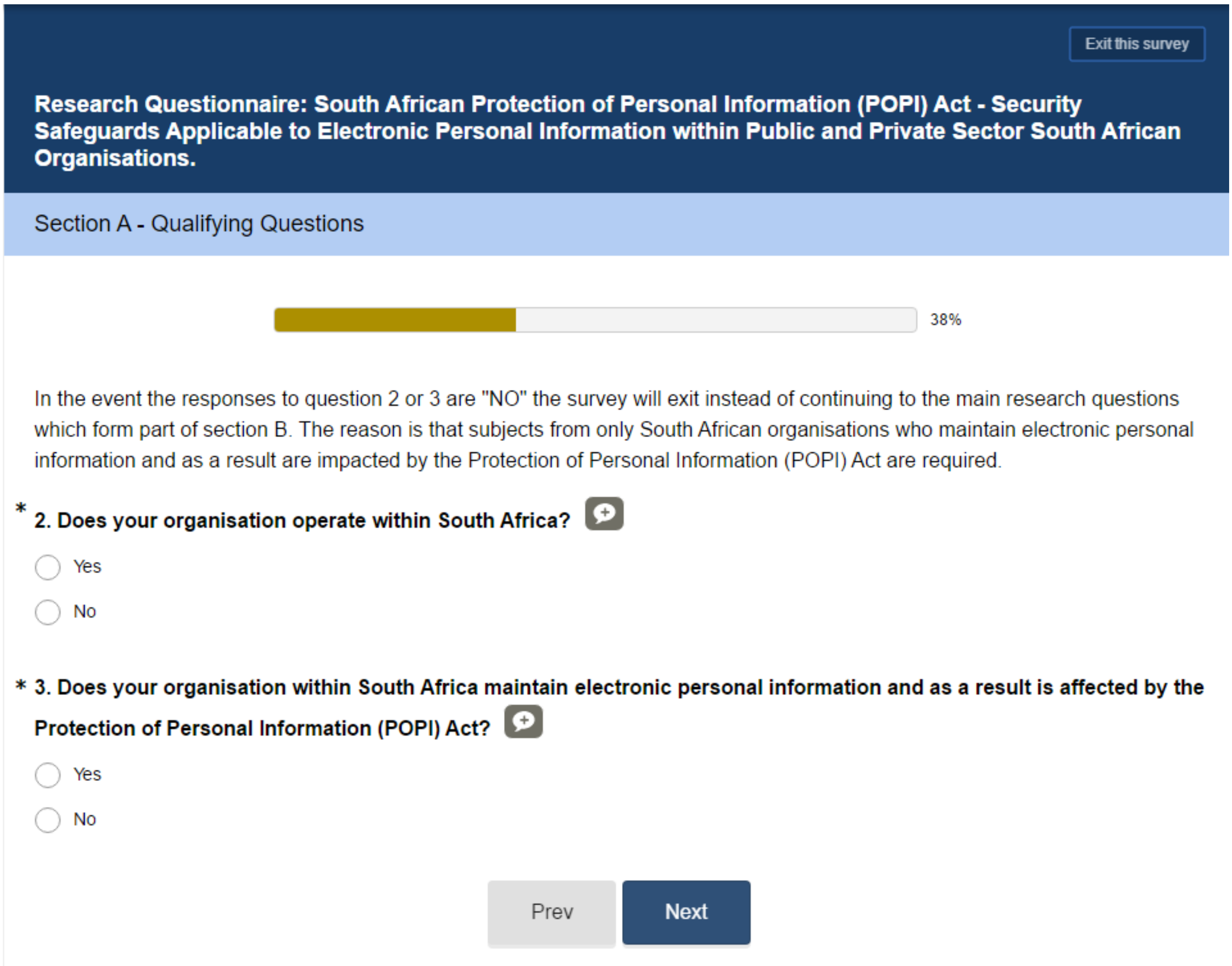
By selecting the "I PROVIDE CONSENT TO COMPLETE THE RESEARCH QUESTIONNAIRE AND ACCEPT THE TERMS AND CONDITIONS STATED ABOVE" option below, you willing provide consent to complete the research questionnaire and understand the terms and conditions stated above.

If you do not want to provide consent to complete the research questionnaire or agree with the terms and conditions stated above, you may press the "EXIT THIS SURVEY" button at the top right hand corner of this page to exit the research questionnaire.

* **1. Consent and Acceptance of Terms and Conditions**

○ I provide consent to complete the research questionnaire and accept the terms and conditions stated above.

APPENDIX D.3 - POPI RESEARCH SURVEY: QUALIFYING QUESTIONS



Research Questionnaire: South African Protection of Personal Information (POPI) Act - Security Safeguards Applicable to Electronic Personal Information within Public and Private Sector South African Organisations.

Section A - Qualifying Questions

In the event the responses to question 2 or 3 are "NO" the survey will exit instead of continuing to the main research questions which form part of section B. The reason is that subjects from only South African organisations who maintain electronic personal information and as a result are impacted by the Protection of Personal Information (POPI) Act are required.

* **2. Does your organisation operate within South Africa?**

○ Yes

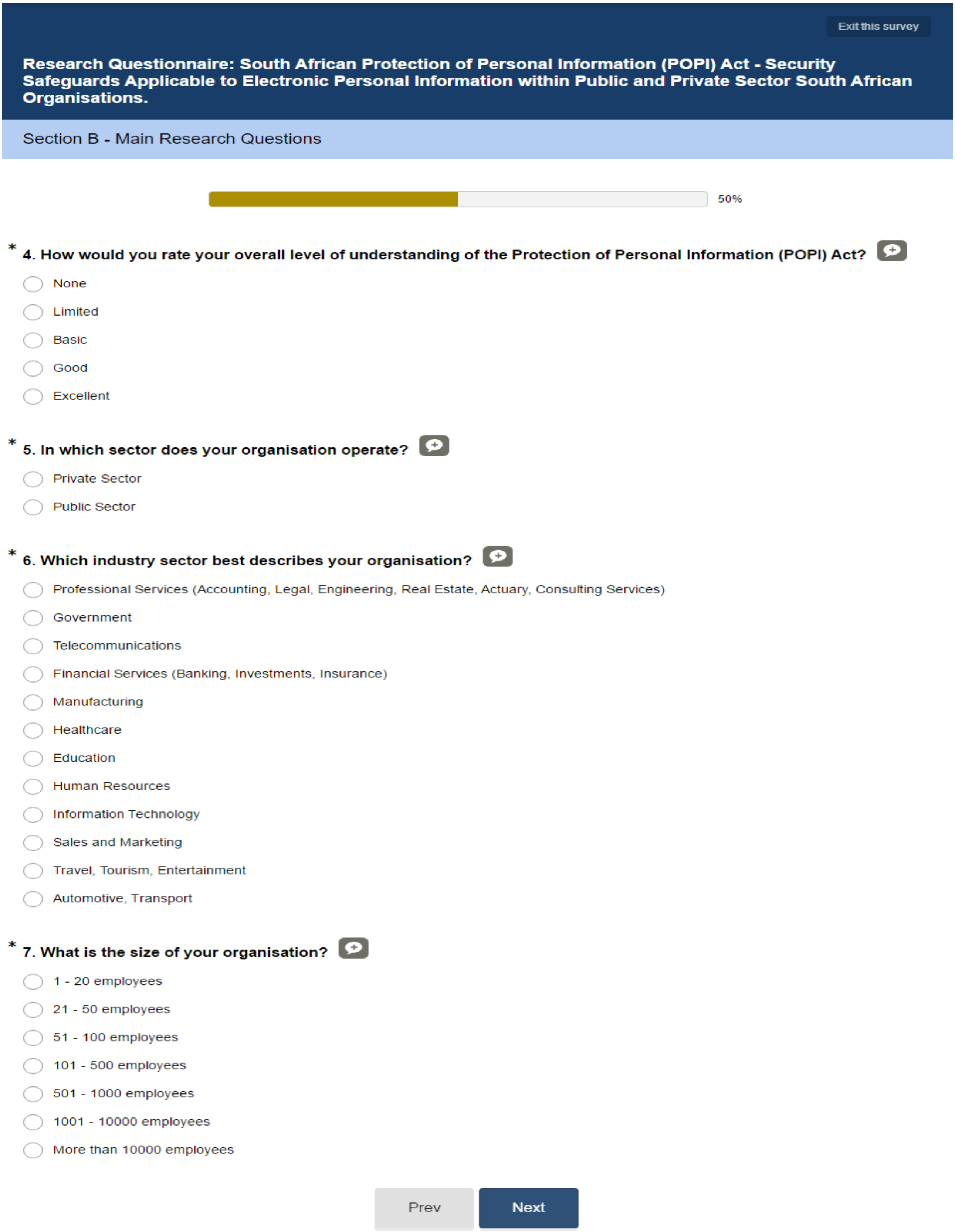
○ No

* **3. Does your organisation within South Africa maintain electronic personal information and as a result is affected by the Protection of Personal Information (POPI) Act?**

○ Yes

○ No

APPENDIX D.4 - POPI RESEARCH SURVEY: MAIN RESEARCH QUESTIONS



Research Questionnaire: South African Protection of Personal Information (POPI) Act - Security Safeguards Applicable to Electronic Personal Information within Public and Private Sector South African Organisations.

Section B - Main Research Questions

* **4. How would you rate your overall level of understanding of the Protection of Personal Information (POPI) Act?**

○ None
○ Limited
○ Basic
○ Good
○ Excellent

* **5. In which sector does your organisation operate?**

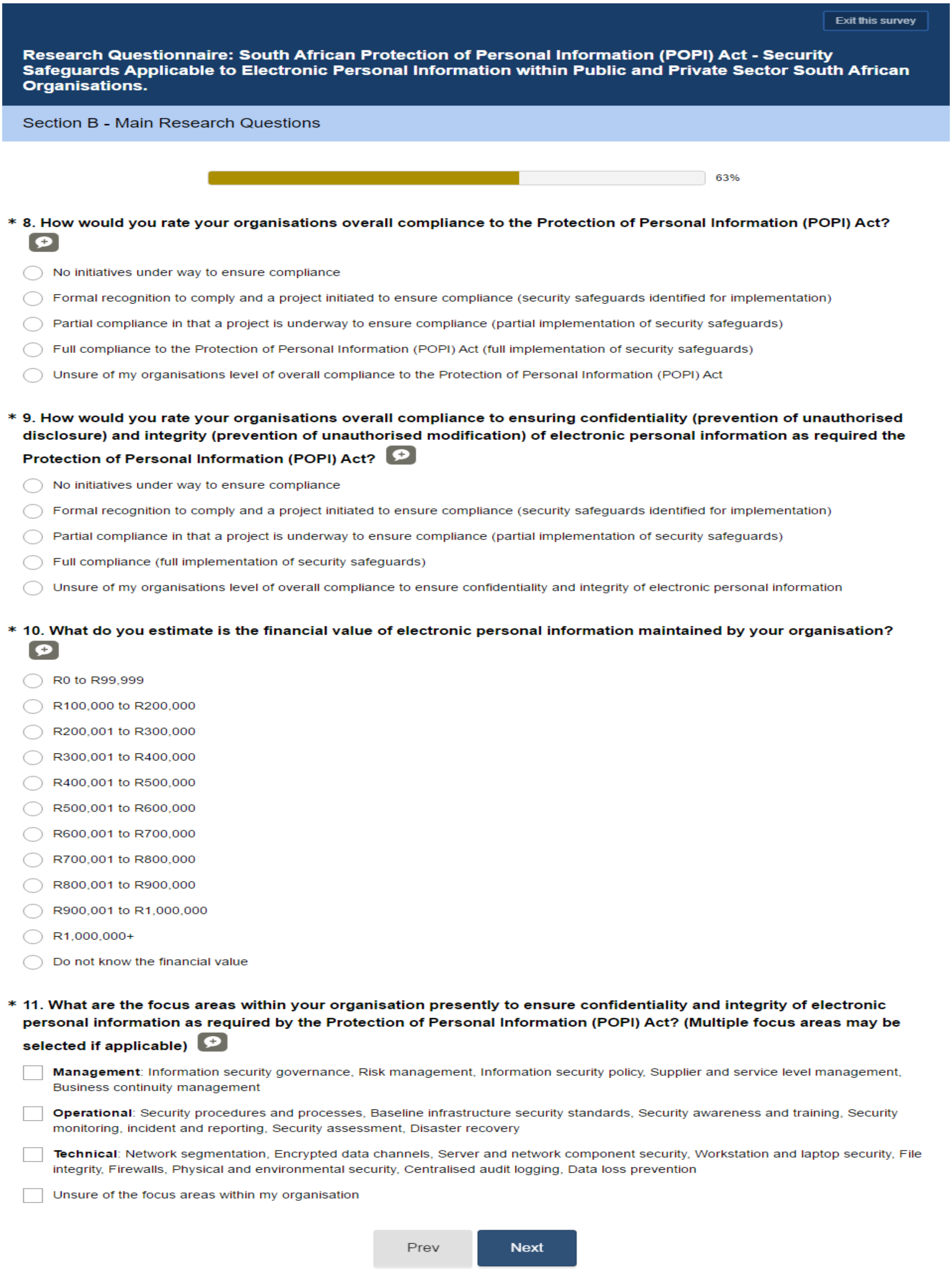
○ Private Sector
○ Public Sector

* **6. Which industry sector best describes your organisation?**

○ Professional Services (Accounting, Legal, Engineering, Real Estate, Actuary, Consulting Services)
○ Government
○ Telecommunications
○ Financial Services (Banking, Investments, Insurance)
○ Manufacturing
○ Healthcare
○ Education
○ Human Resources
○ Information Technology
○ Sales and Marketing
○ Travel, Tourism, Entertainment
○ Automotive, Transport

* **7. What is the size of your organisation?**

○ 1 - 20 employees
○ 21 - 50 employees
○ 51 - 100 employees
○ 101 - 500 employees
○ 501 - 1000 employees
○ 1001 - 10000 employees
○ More than 10000 employees



Research Questionnaire: South African Protection of Personal Information (POPI) Act - Security Safeguards Applicable to Electronic Personal Information within Public and Private Sector South African Organisations.

Section B - Main Research Questions

*** 8. How would you rate your organisations overall compliance to the Protection of Personal Information (POPI) Act?**

○ No initiatives under way to ensure compliance

○ Formal recognition to comply and a project initiated to ensure compliance (security safeguards identified for implementation)

○ Partial compliance in that a project is underway to ensure compliance (partial implementation of security safeguards)

○ Full compliance to the Protection of Personal Information (POPI) Act (full implementation of security safeguards)

○ Unsure of my organisations level of overall compliance to the Protection of Personal Information (POPI) Act

*** 9. How would you rate your organisations overall compliance to ensuring confidentiality (prevention of unauthorised disclosure) and integrity (prevention of unauthorised modification) of electronic personal information as required the Protection of Personal Information (POPI) Act?**

○ No initiatives under way to ensure compliance

○ Formal recognition to comply and a project initiated to ensure compliance (security safeguards identified for implementation)

○ Partial compliance in that a project is underway to ensure compliance (partial implementation of security safeguards)

○ Full compliance (full implementation of security safeguards)

○ Unsure of my organisations level of overall compliance to ensure confidentiality and integrity of electronic personal information

*** 10. What do you estimate is the financial value of electronic personal information maintained by your organisation?**

○ R0 to R99,999

○ R100,000 to R200,000

○ R200,001 to R300,000

○ R300,001 to R400,000

○ R400,001 to R500,000

○ R500,001 to R600,000

○ R600,001 to R700,000

○ R700,001 to R800,000

○ R800,001 to R900,000

○ R900,001 to R1,000,000

○ R1,000,000+

○ Do not know the financial value

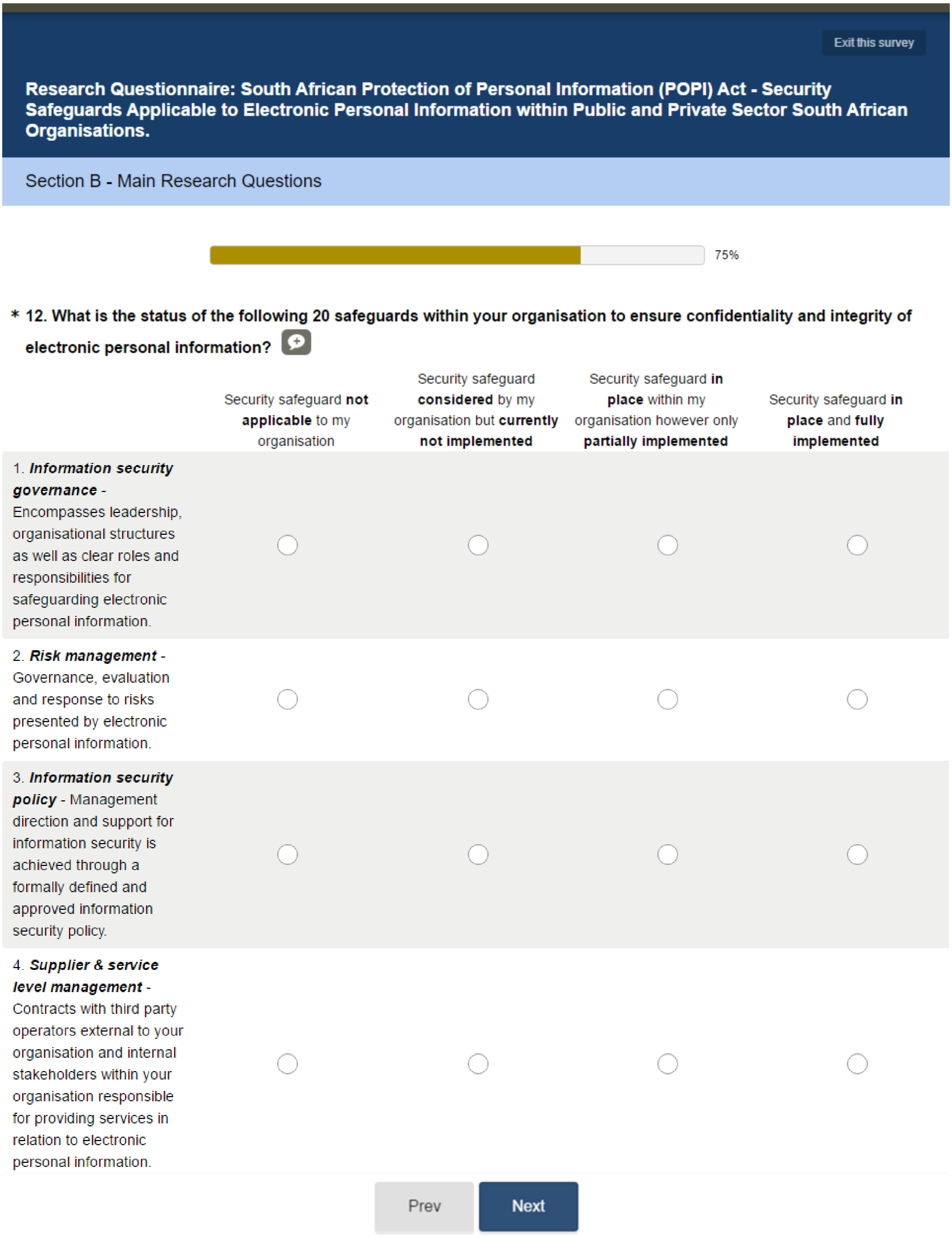
*** 11. What are the focus areas within your organisation presently to ensure confidentiality and integrity of electronic personal information as required by the Protection of Personal Information (POPI) Act? (Multiple focus areas may be selected if applicable)**

□ **Management**: Information security governance, Risk management, Information security policy, Supplier and service level management, Business continuity management

□ **Operational**: Security procedures and processes, Baseline infrastructure security standards, Security awareness and training, Security monitoring, incident and reporting, Security assessment, Disaster recovery

□ **Technical**: Network segmentation, Encrypted data channels, Server and network component security, Workstation and laptop security, File integrity, Firewalls, Physical and environmental security, Centralised audit logging, Data loss prevention

□ Unsure of the focus areas within my organisation

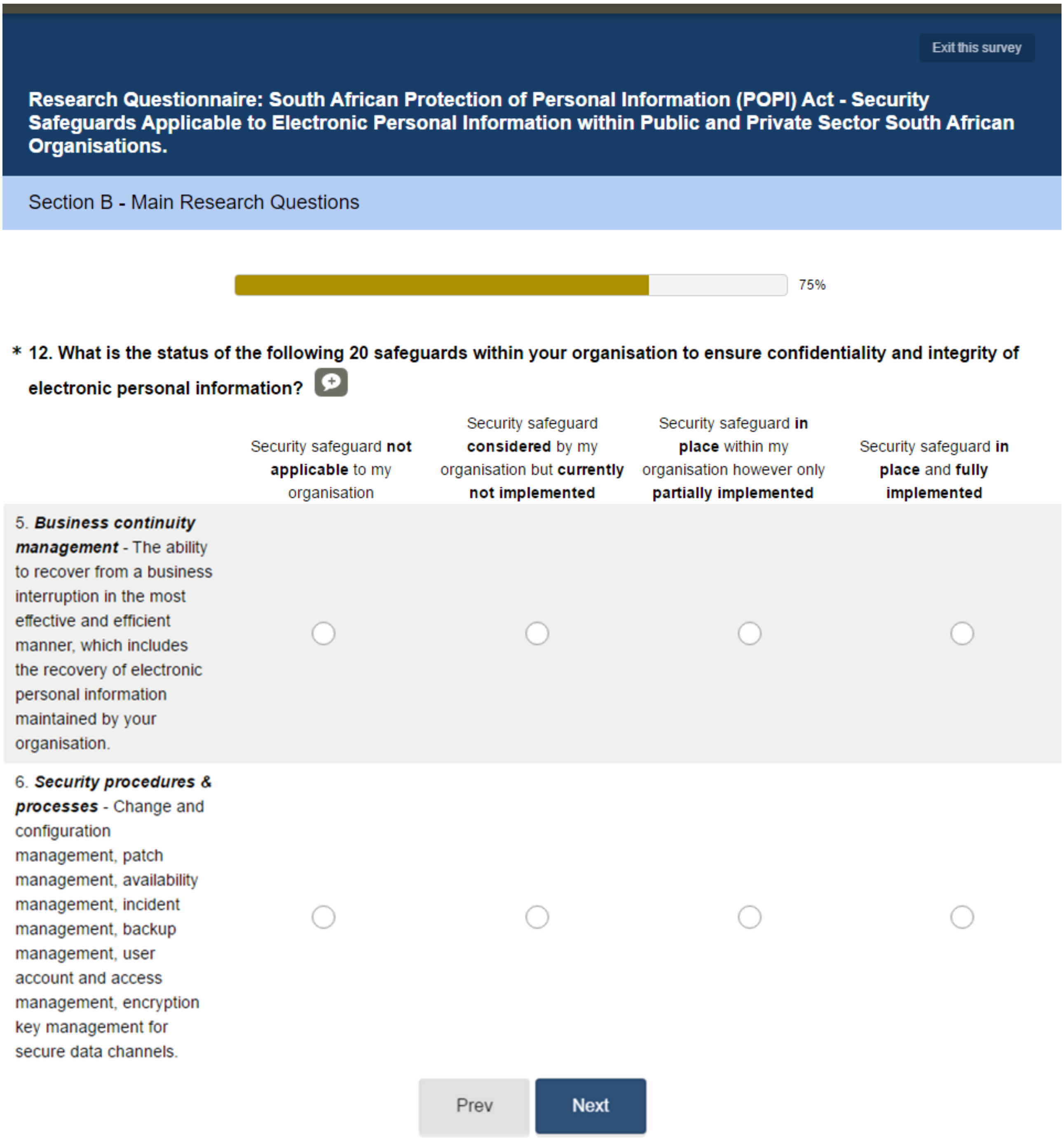


Research Questionnaire: South African Protection of Personal Information (POPI) Act - Security Safeguards Applicable to Electronic Personal Information within Public and Private Sector South African Organisations.

Section B - Main Research Questions

*** 12. What is the status of the following 20 safeguards within your organisation to ensure confidentiality and integrity of electronic personal information?**

	Security safeguard **not applicable** to my organisation	Security safeguard **considered** by my organisation but **currently not implemented**	Security safeguard **in place** within my organisation however only **partially implemented**	Security safeguard **in place** and **fully implemented**
1. ***Information security governance*** - Encompasses leadership, organisational structures as well as clear roles and responsibilities for safeguarding electronic personal information.	○	○	○	○
2. ***Risk management*** - Governance, evaluation and response to risks presented by electronic personal information.	○	○	○	○
3. ***Information security policy*** - Management direction and support for information security is achieved through a formally defined and approved information security policy.	○	○	○	○
4. ***Supplier & service level management*** - Contracts with third party operators external to your organisation and internal stakeholders within your organisation responsible for providing services in relation to electronic personal information.	○	○	○	○



Exit this survey

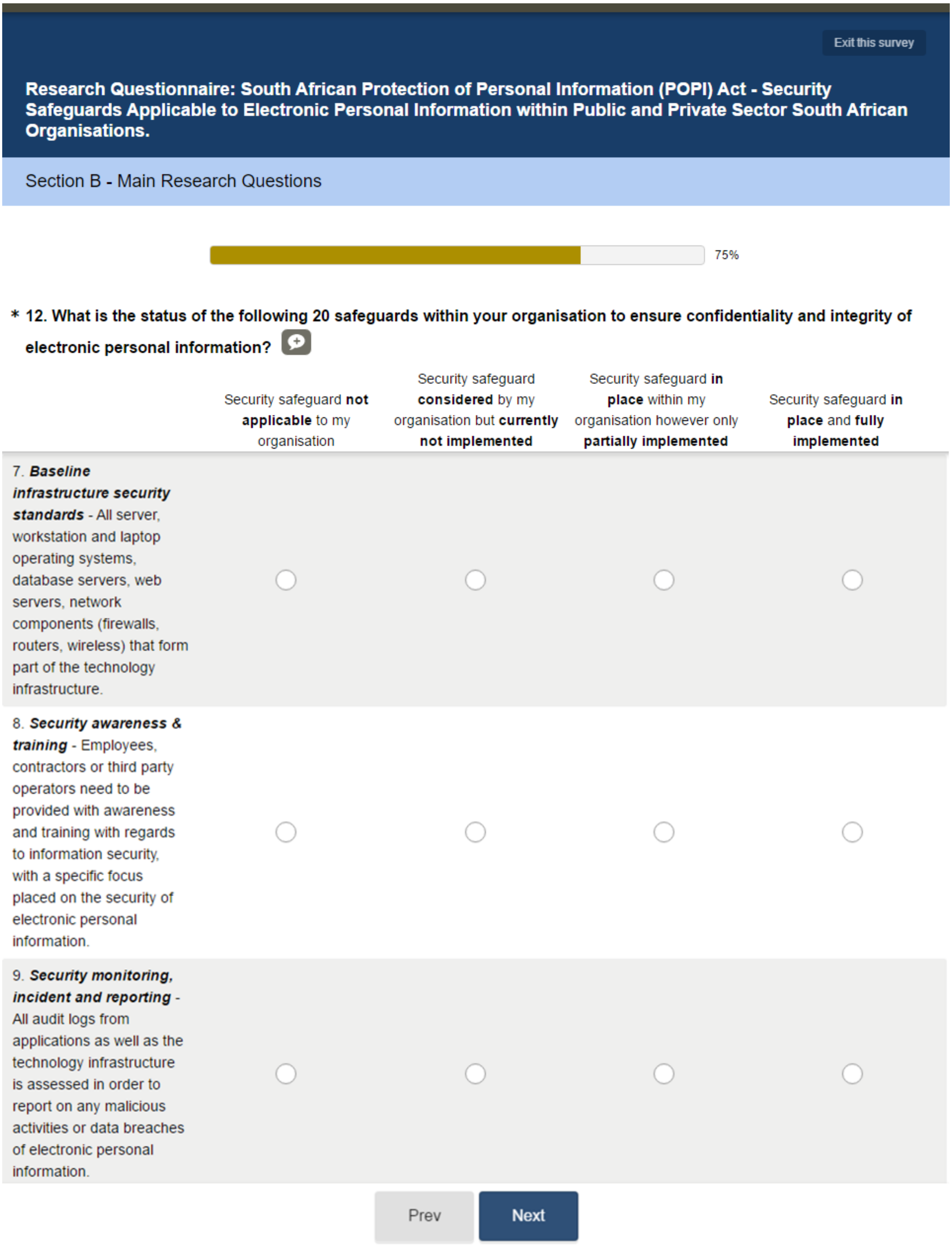
Research Questionnaire: South African Protection of Personal Information (POPI) Act - Security Safeguards Applicable to Electronic Personal Information within Public and Private Sector South African Organisations.

Section B - Main Research Questions

75%

*** 12. What is the status of the following 20 safeguards within your organisation to ensure confidentiality and integrity of electronic personal information?**

	Security safeguard **not applicable** to my organisation	Security safeguard **considered** by my organisation but **currently not implemented**	Security safeguard **in place** within my organisation however only **partially implemented**	Security safeguard **in place** and **fully implemented**
5. ***Business continuity management*** - The ability to recover from a business interruption in the most effective and efficient manner, which includes the recovery of electronic personal information maintained by your organisation.	○	○	○	○
6. ***Security procedures & processes*** - Change and configuration management, patch management, availability management, incident management, backup management, user account and access management, encryption key management for secure data channels.	○	○	○	○



Exit this survey

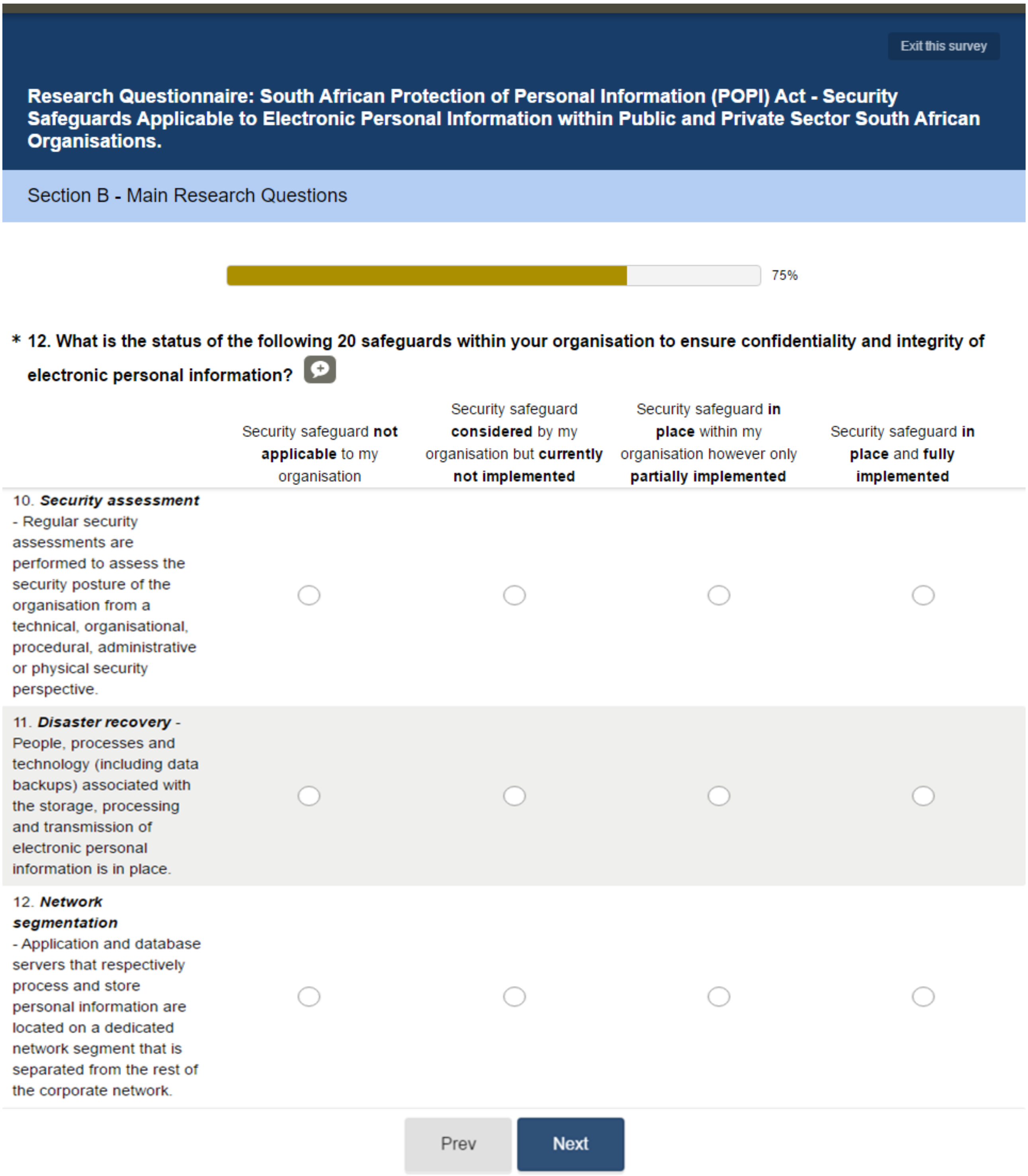
Research Questionnaire: South African Protection of Personal Information (POPI) Act - Security Safeguards Applicable to Electronic Personal Information within Public and Private Sector South African Organisations.

Section B - Main Research Questions

75%

*** 12. What is the status of the following 20 safeguards within your organisation to ensure confidentiality and integrity of electronic personal information?**

	Security safeguard **not applicable** to my organisation	Security safeguard **considered** by my organisation but **currently not implemented**	Security safeguard **in place** within my organisation however only **partially implemented**	Security safeguard **in place** and **fully implemented**
7. ***Baseline infrastructure security standards*** - All server, workstation and laptop operating systems, database servers, web servers, network components (firewalls, routers, wireless) that form part of the technology infrastructure.	○	○	○	○
8. ***Security awareness & training*** - Employees, contractors or third party operators need to be provided with awareness and training with regards to information security, with a specific focus placed on the security of electronic personal information.	○	○	○	○
9. ***Security monitoring, incident and reporting*** - All audit logs from applications as well as the technology infrastructure is assessed in order to report on any malicious activities or data breaches of electronic personal information.	○	○	○	○

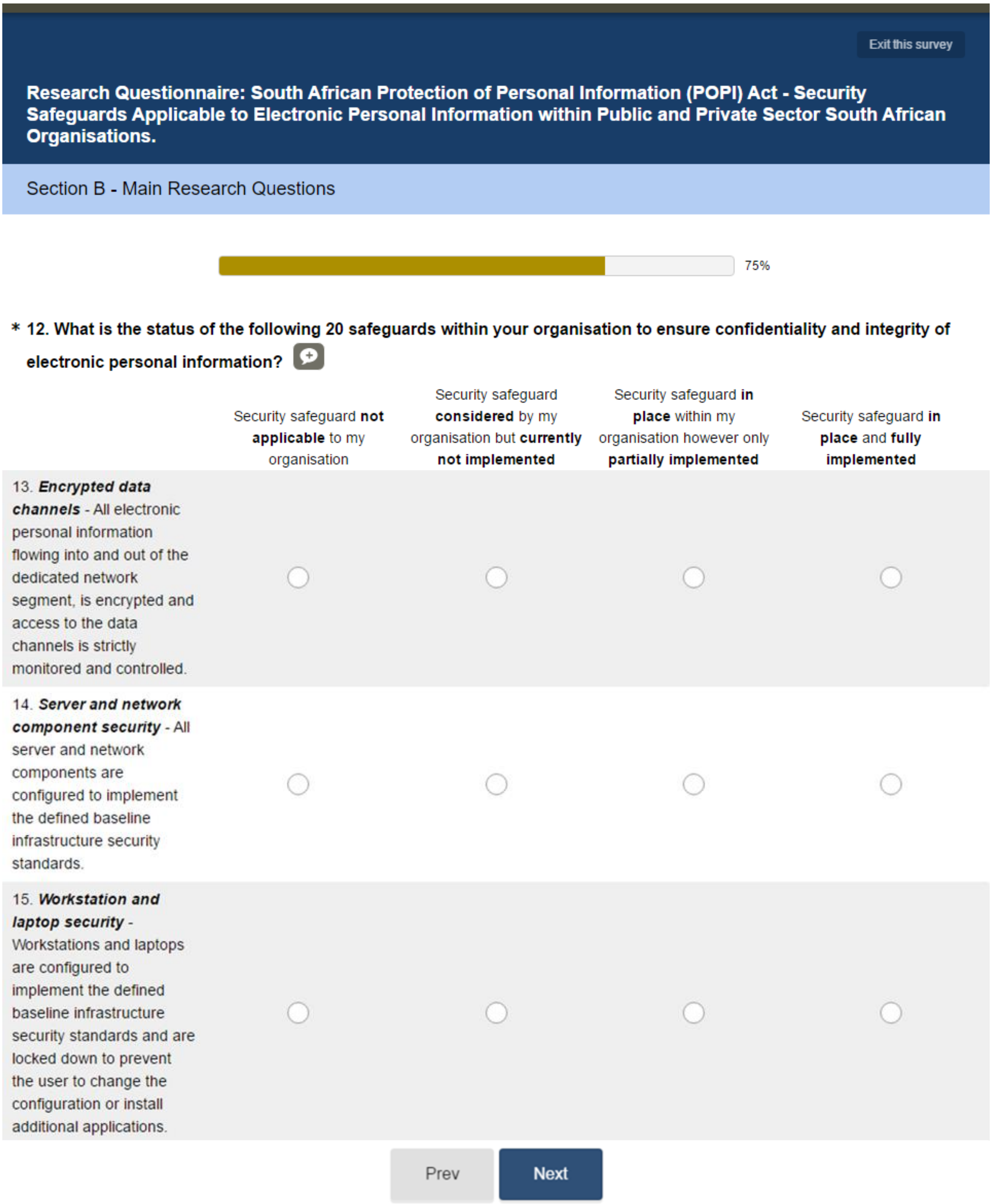


Research Questionnaire: South African Protection of Personal Information (POPI) Act - Security Safeguards Applicable to Electronic Personal Information within Public and Private Sector South African Organisations.

Section B - Main Research Questions

*** 12. What is the status of the following 20 safeguards within your organisation to ensure confidentiality and integrity of electronic personal information?**

	Security safeguard **not applicable** to my organisation	Security safeguard **considered** by my organisation but **currently not implemented**	Security safeguard **in place** within my organisation however only **partially implemented**	Security safeguard **in place** and **fully implemented**
10. ***Security assessment*** - Regular security assessments are performed to assess the security posture of the organisation from a technical, organisational, procedural, administrative or physical security perspective.	○	○	○	○
11. ***Disaster recovery*** - People, processes and technology (including data backups) associated with the storage, processing and transmission of electronic personal information is in place.	○	○	○	○
12. ***Network segmentation*** - Application and database servers that respectively process and store personal information are located on a dedicated network segment that is separated from the rest of the corporate network.	○	○	○	○

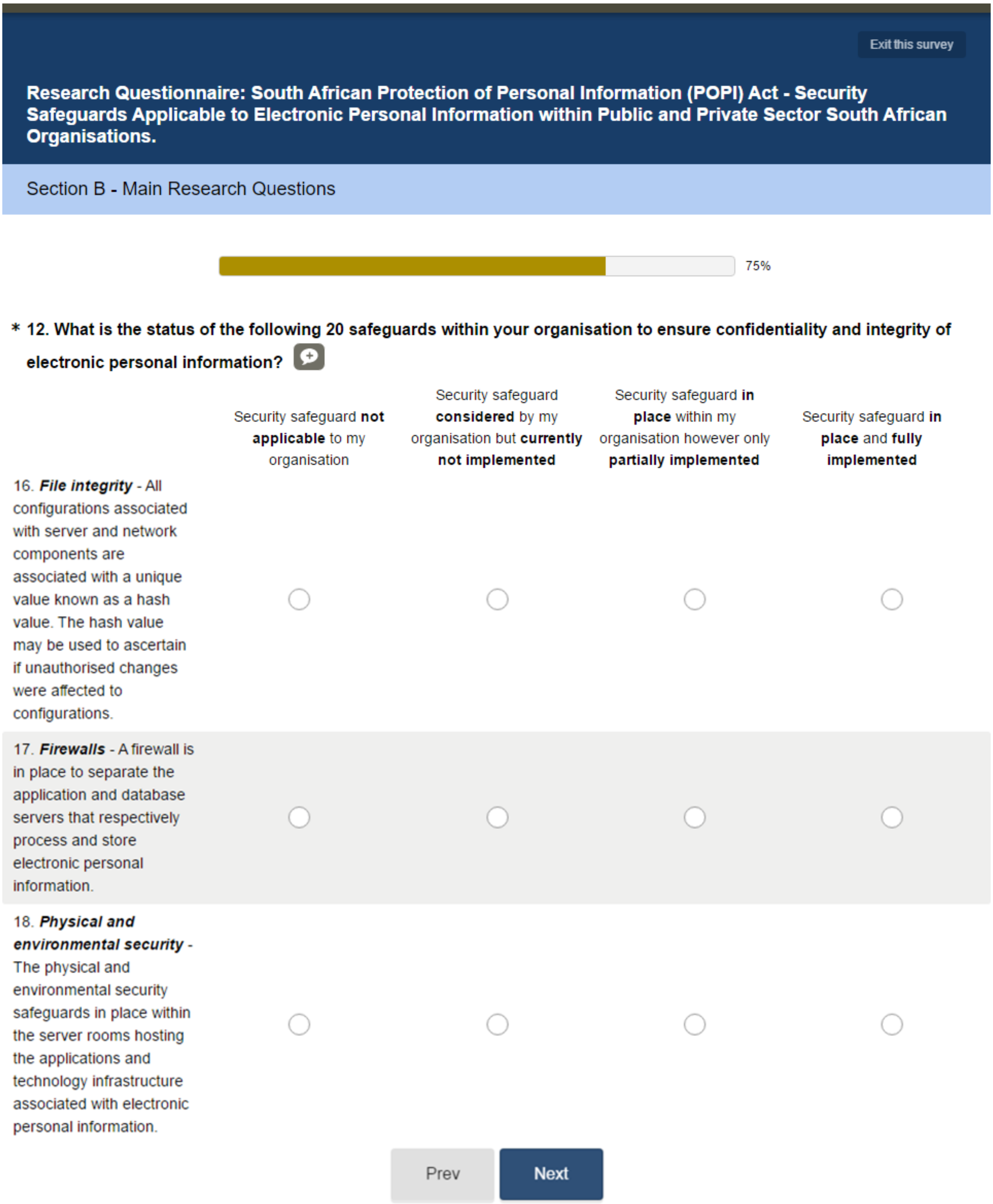


Research Questionnaire: South African Protection of Personal Information (POPI) Act - Security Safeguards Applicable to Electronic Personal Information within Public and Private Sector South African Organisations.

Section B - Main Research Questions

*** 12. What is the status of the following 20 safeguards within your organisation to ensure confidentiality and integrity of electronic personal information?**

	Security safeguard **not applicable** to my organisation	Security safeguard **considered** by my organisation but **currently not implemented**	Security safeguard **in place** within my organisation however only **partially implemented**	Security safeguard **in place** and **fully implemented**
13. ***Encrypted data channels*** - All electronic personal information flowing into and out of the dedicated network segment, is encrypted and access to the data channels is strictly monitored and controlled.	○	○	○	○
14. ***Server and network component security*** - All server and network components are configured to implement the defined baseline infrastructure security standards.	○	○	○	○
15. ***Workstation and laptop security*** - Workstations and laptops are configured to implement the defined baseline infrastructure security standards and are locked down to prevent the user to change the configuration or install additional applications.	○	○	○	○

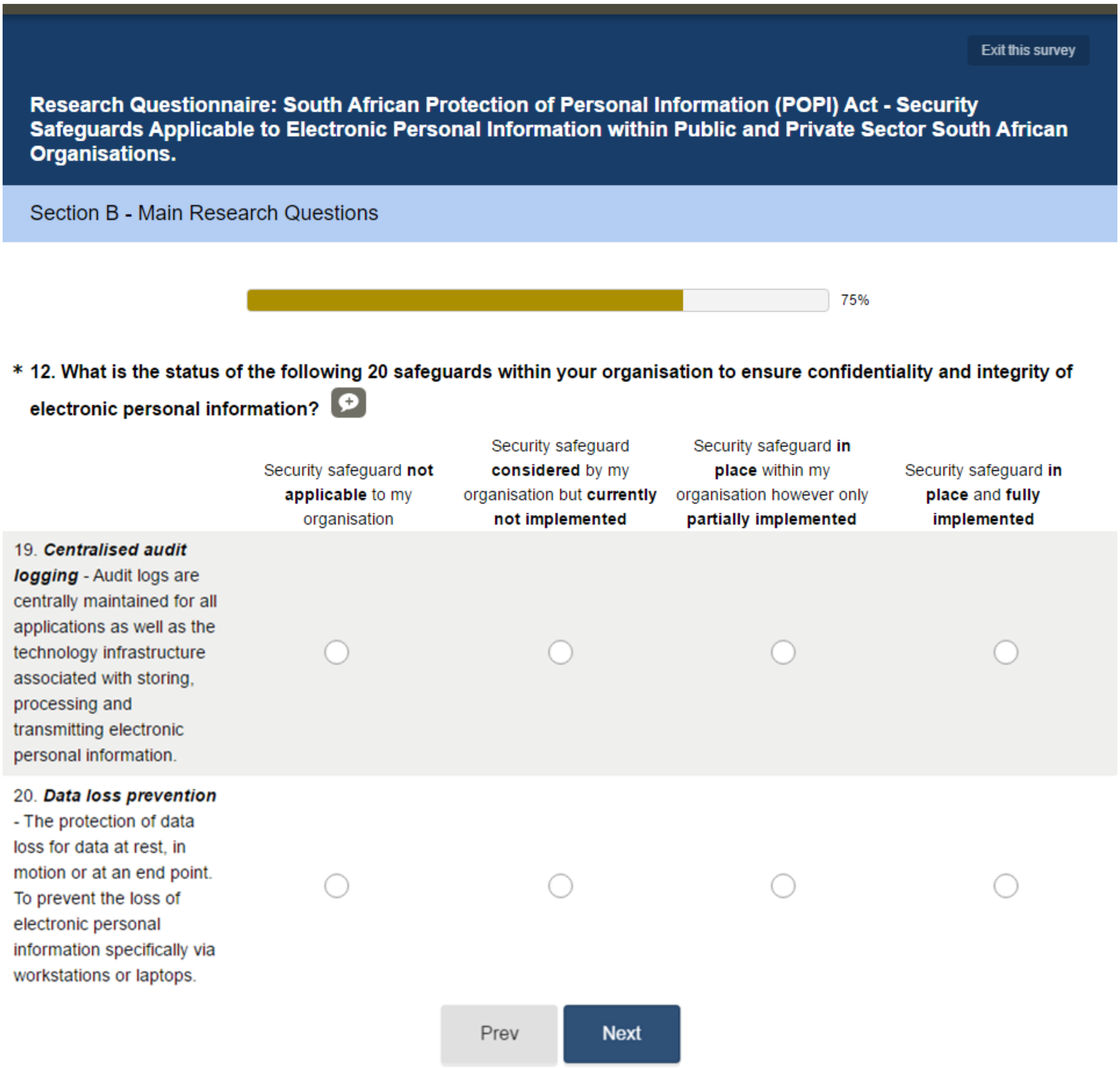


Research Questionnaire: South African Protection of Personal Information (POPI) Act - Security Safeguards Applicable to Electronic Personal Information within Public and Private Sector South African Organisations.

Section B - Main Research Questions

*** 12. What is the status of the following 20 safeguards within your organisation to ensure confidentiality and integrity of electronic personal information?**

	Security safeguard **not applicable** to my organisation	Security safeguard **considered** by my organisation but **currently not implemented**	Security safeguard **in place** within my organisation however only **partially implemented**	Security safeguard **in place** and **fully implemented**
16. ***File integrity*** - All configurations associated with server and network components are associated with a unique value known as a hash value. The hash value may be used to ascertain if unauthorised changes were affected to configurations.	○	○	○	○
17. ***Firewalls*** - A firewall is in place to separate the application and database servers that respectively process and store electronic personal information.	○	○	○	○
18. ***Physical and environmental security*** - The physical and environmental security safeguards in place within the server rooms hosting the applications and technology infrastructure associated with electronic personal information.	○	○	○	○

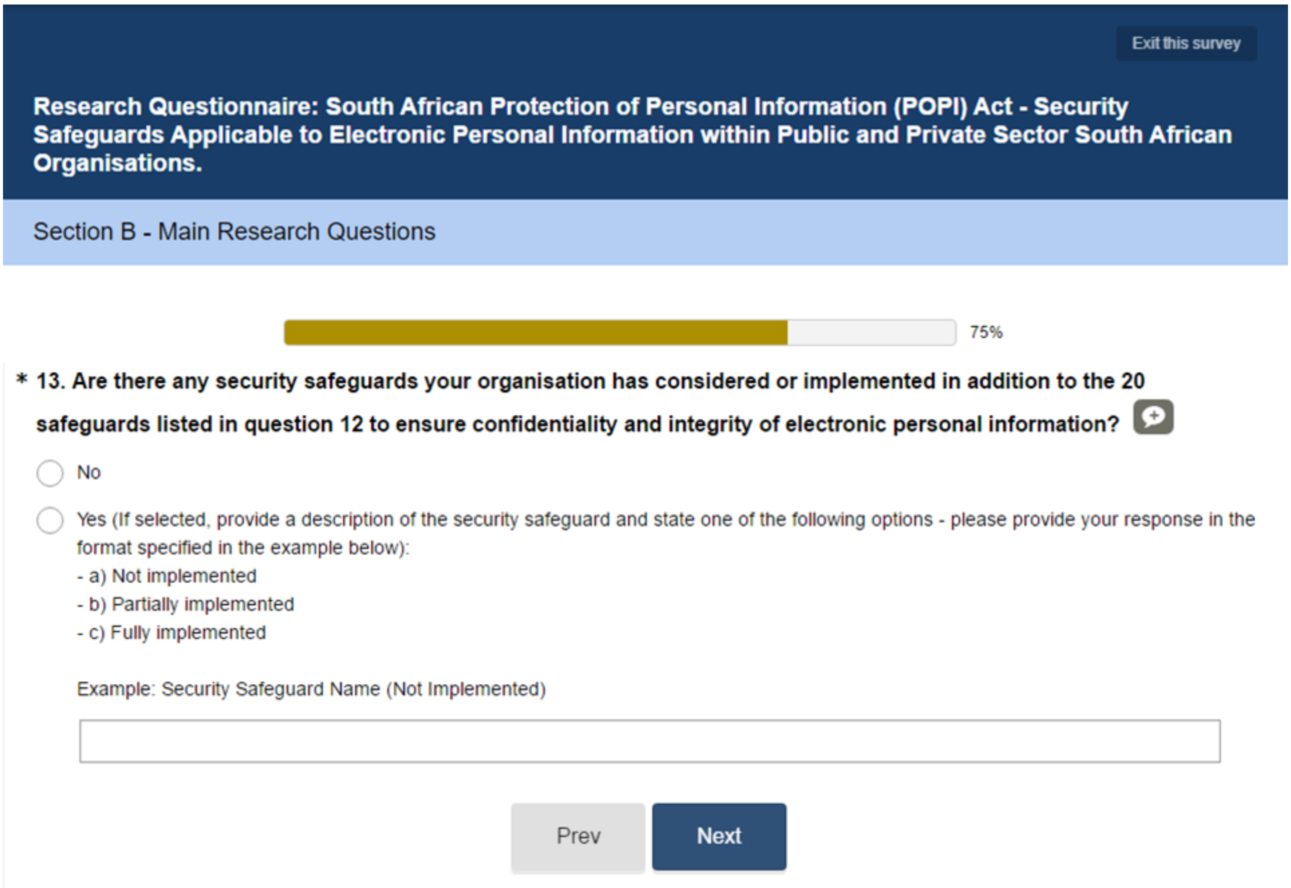


Research Questionnaire: South African Protection of Personal Information (POPI) Act - Security Safeguards Applicable to Electronic Personal Information within Public and Private Sector South African Organisations.

Section B - Main Research Questions

*** 12. What is the status of the following 20 safeguards within your organisation to ensure confidentiality and integrity of electronic personal information?**

	Security safeguard **not applicable** to my organisation	Security safeguard **considered** by my organisation but **currently not implemented**	Security safeguard **in place** within my organisation however only **partially implemented**	Security safeguard **in place** and **fully implemented**
19. ***Centralised audit logging*** - Audit logs are centrally maintained for all applications as well as the technology infrastructure associated with storing, processing and transmitting electronic personal information.	○	○	○	○
20. ***Data loss prevention*** - The protection of data loss for data at rest, in motion or at an end point. To prevent the loss of electronic personal information specifically via workstations or laptops.	○	○	○	○



Research Questionnaire: South African Protection of Personal Information (POPI) Act - Security Safeguards Applicable to Electronic Personal Information within Public and Private Sector South African Organisations.

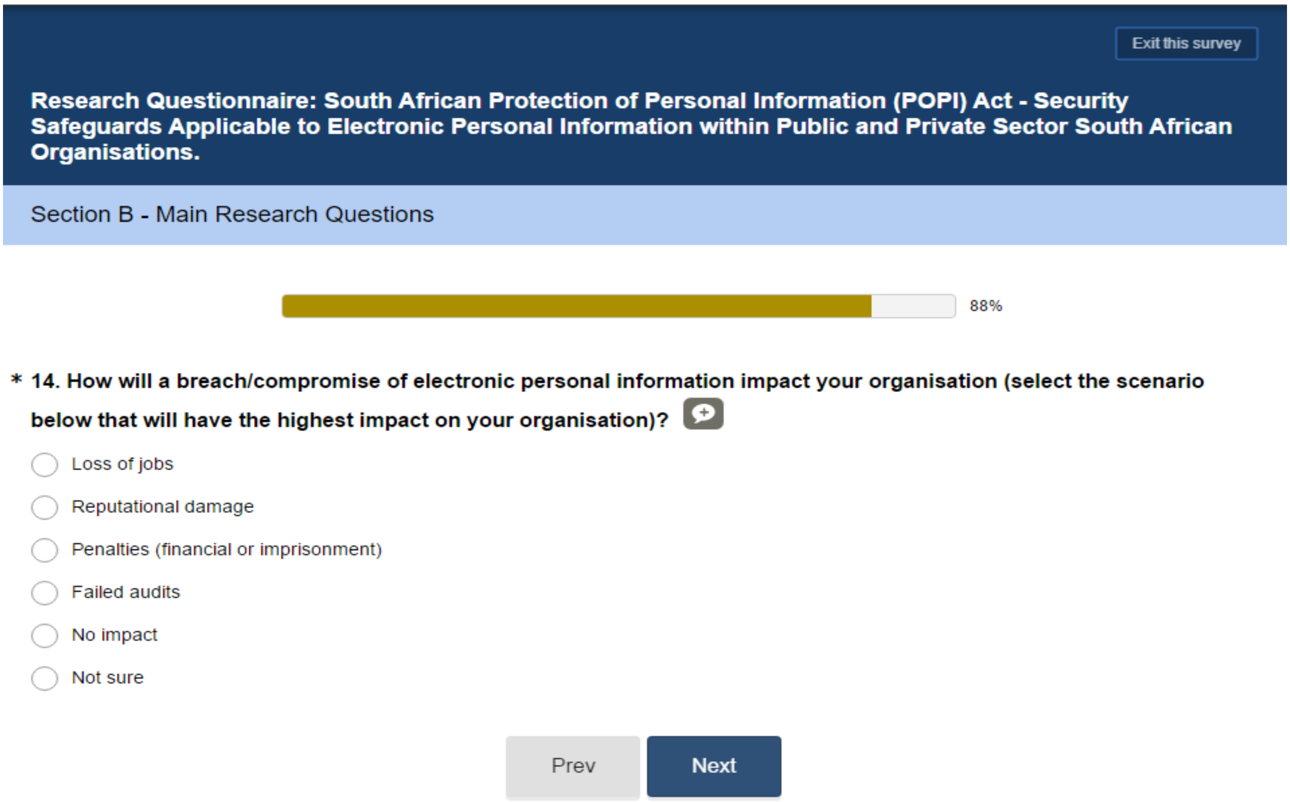
Section B - Main Research Questions

*** 13. Are there any security safeguards your organisation has considered or implemented in addition to the 20 safeguards listed in question 12 to ensure confidentiality and integrity of electronic personal information?**

○ No

○ Yes (If selected, provide a description of the security safeguard and state one of the following options - please provide your response in the format specified in the example below):
- a) Not implemented
- b) Partially implemented
- c) Fully implemented

Example: Security Safeguard Name (Not Implemented)



Research Questionnaire: South African Protection of Personal Information (POPI) Act - Security Safeguards Applicable to Electronic Personal Information within Public and Private Sector South African Organisations.

Section B - Main Research Questions

*** 14. How will a breach/compromise of electronic personal information impact your organisation (select the scenario below that will have the highest impact on your organisation)?**

○ Loss of jobs

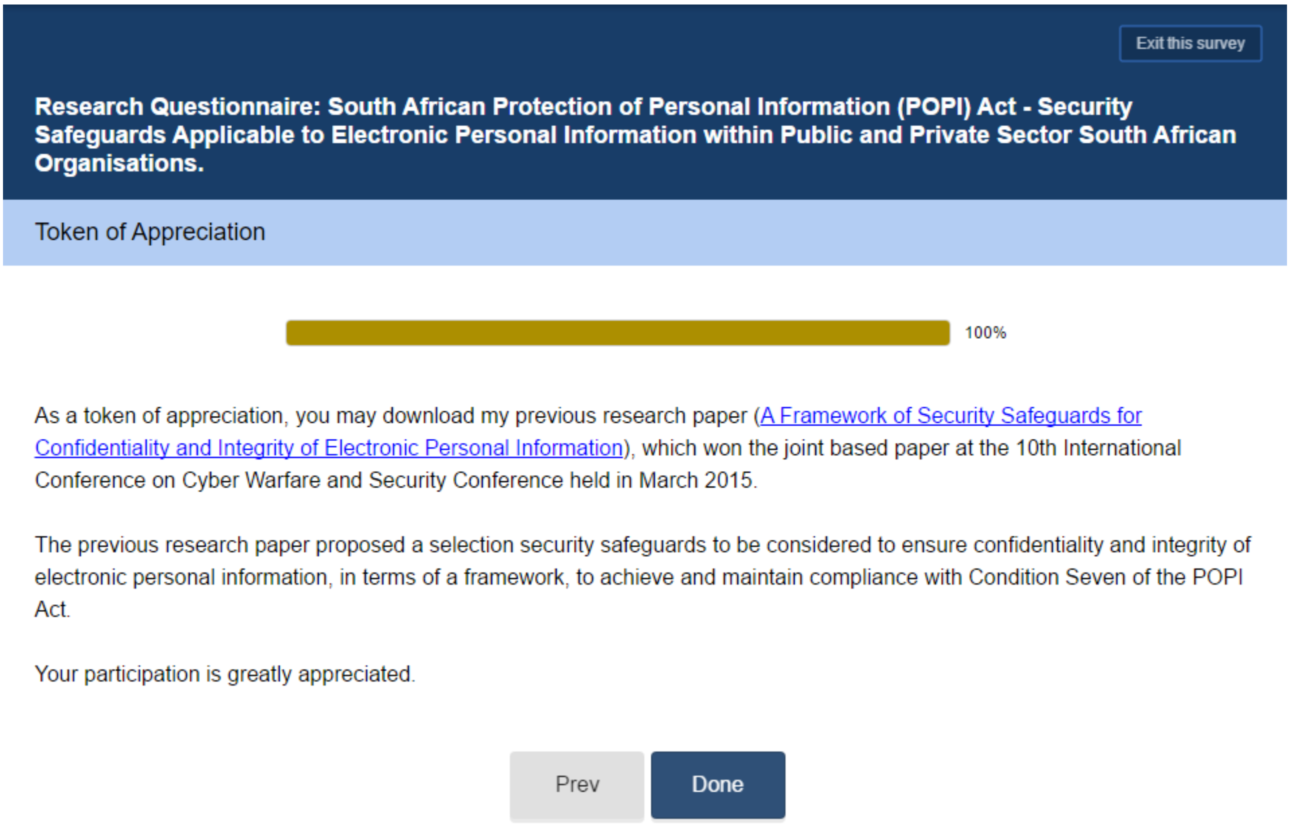
○ Reputational damage

○ Penalties (financial or imprisonment)

○ Failed audits

○ No impact

○ Not sure



Research Questionnaire: South African Protection of Personal Information (POPI) Act - Security Safeguards Applicable to Electronic Personal Information within Public and Private Sector South African Organisations.

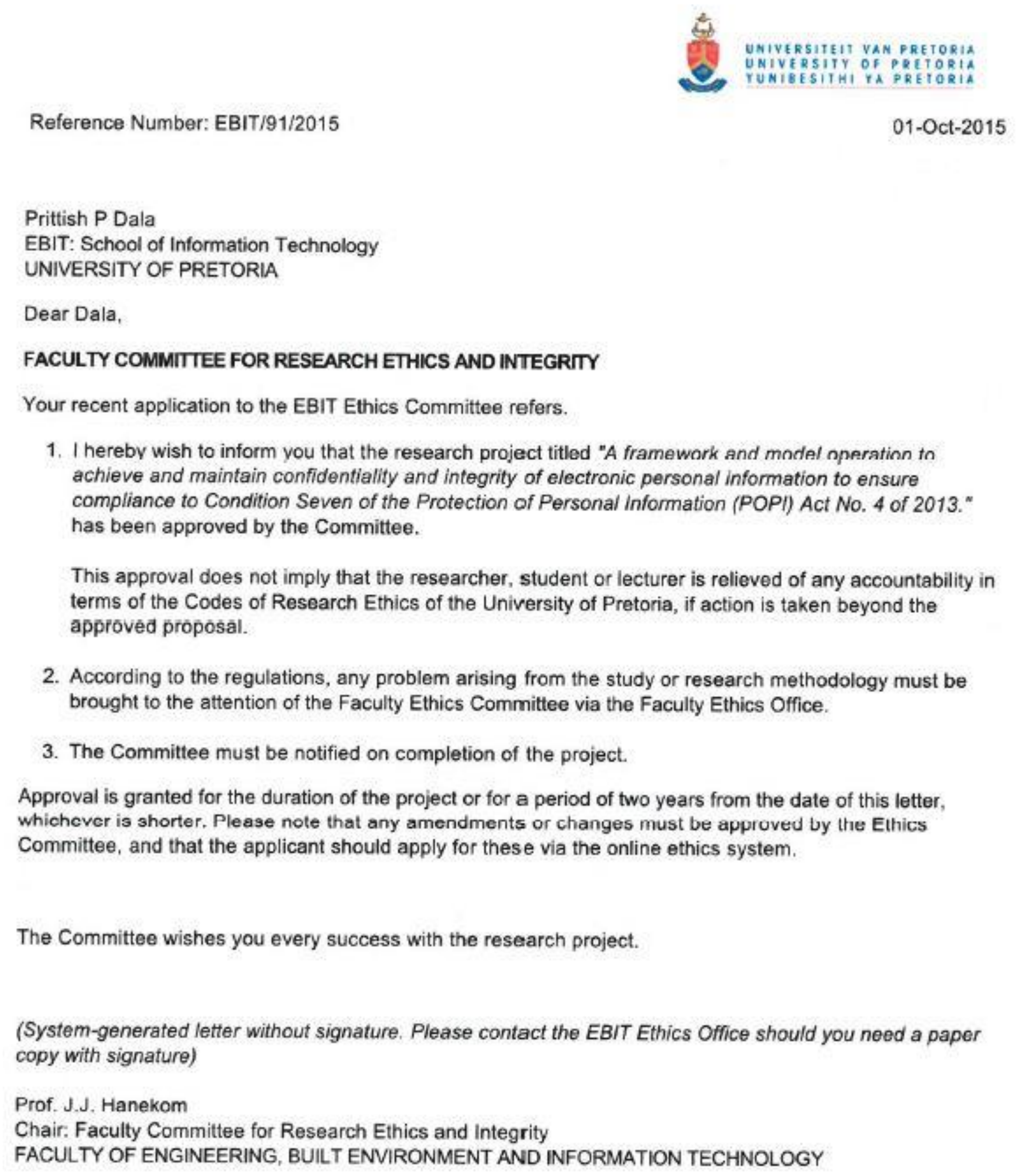
Token of Appreciation

As a token of appreciation, you may download my previous research paper (A Framework of Security Safeguards for Confidentiality and Integrity of Electronic Personal Information), which won the joint based paper at the 10th International Conference on Cyber Warfare and Security Conference held in March 2015.

The previous research paper proposed a selection security safeguards to be considered to ensure confidentiality and integrity of electronic personal information, in terms of a framework, to achieve and maintain compliance with Condition Seven of the POPI Act.

Your participation is greatly appreciated.

APPENDIX E - ETHICS COMMITTEE APPROVAL



UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

Reference Number: EBIT/91/2015

01-Oct-2015

Prittish P Dala
EBIT: School of Information Technology
UNIVERSITY OF PRETORIA

Dear Dala,

FACULTY COMMITTEE FOR RESEARCH ETHICS AND INTEGRITY

Your recent application to the EBIT Ethics Committee refers.

1. I hereby wish to inform you that the research project titled *"A framework and model operation to achieve and maintain confidentiality and integrity of electronic personal information to ensure compliance to Condition Seven of the Protection of Personal Information (POPI) Act No. 4 of 2013."* has been approved by the Committee.

   This approval does not imply that the researcher, student or lecturer is relieved of any accountability in terms of the Codes of Research Ethics of the University of Pretoria, if action is taken beyond the approved proposal.

2. According to the regulations, any problem arising from the study or research methodology must be brought to the attention of the Faculty Ethics Committee via the Faculty Ethics Office.

3. The Committee must be notified on completion of the project.

Approval is granted for the duration of the project or for a period of two years from the date of this letter, whichever is shorter. Please note that any amendments or changes must be approved by the Ethics Committee, and that the applicant should apply for these via the online ethics system.

The Committee wishes you every success with the research project.

(System-generated letter without signature. Please contact the EBIT Ethics Office should you need a paper copy with signature)

Prof. J.J. Hanekom
Chair: Faculty Committee for Research Ethics and Integrity
FACULTY OF ENGINEERING, BUILT ENVIRONMENT AND INFORMATION TECHNOLOGY

APPENDIX F - RESEARCH PUBLICATIONS

University of Venda

CSIR
our future through science

Proceedings of the 10th International Conference on Cyber Warfare and Security

Co-hosted by
The University of Venda
and
The Council for Scientific and Industrial Research
Kruger National Park
South Africa

24-25 March 2015

Edited by
Dr Jannie Zaaiman
University of Venda, South Africa
and
Dr Louise Leenen
Council for Scientific and Industrial Research, South Africa

acpi

A conference managed by ACPI, UK

Proceedings of
The 10th International Conference on
Cyber Warfare and Security
ICCWS-2015

Co-hosted by the
University of Venda
and
The Council for Scientific and Industrial Research
Kruger National Park
South Africa

24-25 March 2015

Edited by
Dr Jannie Zaaiman
And
Dr Louise Leenen

Papers have been double-blind peer reviewed before final submission to the conference. Initially, paper abstracts were read and selected by the conference panel for submission as possible papers for the conference.

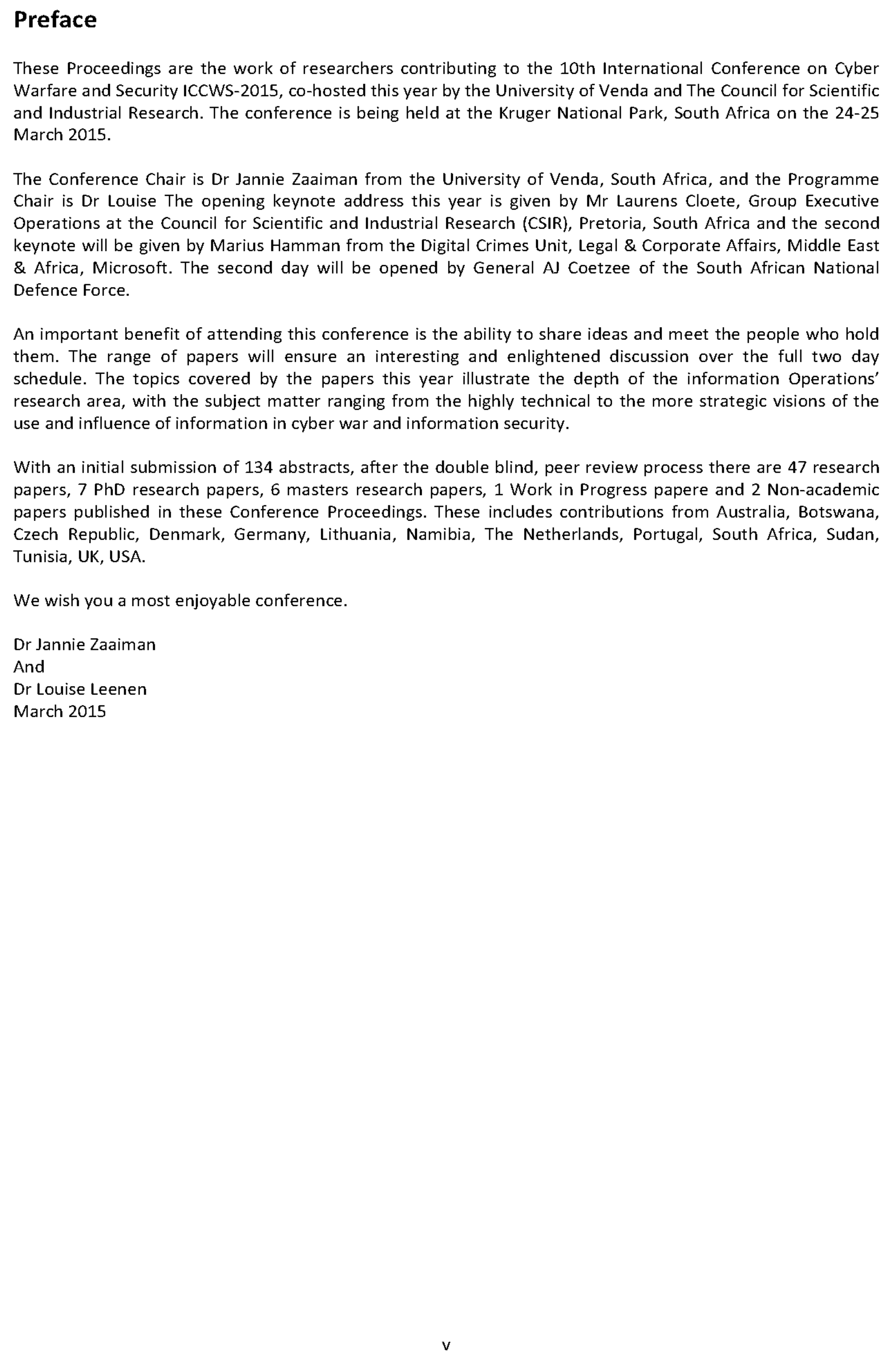
Many thanks to the reviewers who helped ensure the quality of the full papers.

These Conference Proceedings have been submitted to Thomson ISI for indexing.

Further copies of this book and previous year's proceedings can be purchased from http://academic-bookshop.com

E-Book ISBN: 978-1-910309-97-1
E-Book ISSN: 2048-9889
Book version ISBN: 978-1-910309-96-4
Book Version ISSN: 2048-9870
CD Version ISBN: 978-1-910309-98-8
CD Version ISSN: 2048-9897

Published by Academic Conferences and Publishing International Limited
Reading
UK
44-118-972-4148
www.academic-publishing.org



Preface

These Proceedings are the work of researchers contributing to the 10th International Conference on Cyber Warfare and Security ICCWS-2015, co-hosted this year by the University of Venda and The Council for Scientific and Industrial Research. The conference is being held at the Kruger National Park, South Africa on the 24-25 March 2015.

The Conference Chair is Dr Jannie Zaaiman from the University of Venda, South Africa, and the Programme Chair is Dr Louise The opening keynote address this year is given by Mr Laurens Cloete, Group Executive Operations at the Council for Scientific and Industrial Research (CSIR), Pretoria, South Africa and the second keynote will be given by Marius Hamman from the Digital Crimes Unit, Legal & Corporate Affairs, Middle East & Africa, Microsoft. The second day will be opened by General AJ Coetzee of the South African National Defence Force.

An important benefit of attending this conference is the ability to share ideas and meet the people who hold them. The range of papers will ensure an interesting and enlightened discussion over the full two day schedule. The topics covered by the papers this year illustrate the depth of the information Operations' research area, with the subject matter ranging from the highly technical to the more strategic visions of the use and influence of information in cyber war and information security.

With an initial submission of 134 abstracts, after the double blind, peer review process there are 47 research papers, 7 PhD research papers, 6 masters research papers, 1 Work in Progress papere and 2 Non-academic papers published in these Conference Proceedings. These includes contributions from Australia, Botswana, Czech Republic, Denmark, Germany, Lithuania, Namibia, The Netherlands, Portugal, South Africa, Sudan, Tunisia, UK, USA.

We wish you a most enjoyable conference.

Dr Jannie Zaaiman
And
Dr Louise Leenen
March 2015

Conference Committee

Conference Executive

Dr Jannie Zaaiman, University of Venda, South Africa
Dr Louise Leenen, Council for Scientific and Industrial Research, South Africa
Joey Jansen van Vuuren, Council for Scientific and Industrial Research
Suné von Solms, Council for Scientific and Industrial Research, South Africa
Brett van Niekerk, University of KwaZulu-Natal, South Africa

Mini track chairs:
Dr John S. Hurley, Defense University (NDU) iCollege, USA
Dr John McCarthy, Airport CyberSec division, ServiceTec, UK

Committee Members
The conference programme committee consists of key people in the information systems, information warfare and information security communities around the world. The following people have confirmed their participation:

Dr. Kareem Kamal A.Ghany (Faculty of Computers & Information, Egypt); Abukari Abdul Hanan (University For Development Studies, Ghana); Prof Azween Abdullah (Malaysian University if Science and Technology, Malaysia); Dr. Bulent Acma (Anadolu University, Eskisehir, Turkey); Dr. William Acosta (University of Toledo, USA); Gail-joon Ahn (University of North Carolina at Charlotte, USA); Dr. Todd Andel (University of South Alabama, USA); Dr. Leigh Armistead (Edith Cowan University, Australia); Johnnes Arreymbi (University of East London, UK); Prof. Richard Baskerville (Georgia State University, USA); Prof. Alexander Bligh (Ariel University Center, Ariel, Israel); Dr. Svet Braynov (University of Illinois, Springfield, USA); Dr. Raymond Buettner (Naval Postgraduate School, USA); Ivan Burke (CSIR, Pretoria, South Africa); Dr. Jonathan Butts (AFIT, USA); Ass Prof. Marco Carvalho (Florida Institute of Technology, USA); Dr. Joobin Choobineh (Texas A&M University, USA); Prof. Sam Chung (University of Washington, Tacoma, USA); Dr. Nathan Clarke (University of Plymouth, UK); Dr. Ronen Cohen (Ariel University Centre, Israel); Earl Crane (George Washington University, USA); Dr. Michael Dahan (Sapir College, Israel); Geoffrey Darnton (Requirements Analytics., UK); Dr. Dipankar Dasgupta (Intelligent Security Systems Research Lab, University of Memphis, USA); Evan Dembskey (UNISA, South Africa); Dorothy Denning (Naval Post Graduate School, USA); jayanthila Devi (Anna university, India); Dr. Glenn Dietrich (University of Texas, Antonio, USA); Prokopios Drogkaris (University of the Aegean, Greece); Barbara Endicott-Popovsky (Center for Information Assurance and Cybersecurity, University of Washington, Seattle,, USA); Prof. Dr. Alptekin Erkollar (ETCOP, Austria); Dr. Cris Ewell (Seattle Children's, USA); Dr Christophe Feltus (Public Research Centre Henri Tudor, Luxembourg); Larry Fleurantin (Larry R. Fleurantin & Associates, P.A., USA); Kenneth Geers (Cooperative Cyber Defence Centre of Excellence, USA); Dr Ahmad Ghafarian (University of North Georgia, USA); Prof. Klaus-Gerd Giesen (Université d'Auvergne, France); Kevin Gleason (KMG Consulting, MA, USA); Dr. Samiksha Godara (Shamsher Bahadur Saxena College Of Law, India); Prof. Dr. Tim Grant (Retired But Active Researcher, Netherlands., The Netherlands); Mr. Murray Greg (Department of Navy , USA); Virginia Greiman (Boston University, USA); Dr. Michael Grimaila (Air Force Institute of Technology, USA); Daniel Grosu (Wayne State University, Detroit, USA, USA); Dr ALASADI HAMID (Basra University, Iraq); Dr. Drew Hamilton (Mississippi State University, USA); Joel Harding (IO Institute, Association of Old Crows, USA); Dr. Douglas Hart (Regis University, USA); Dr. Dwight Haworth (University of Nebraska at Omaha, USA); Michael Henson (Thayer School of Engineering at Dartmouth College, Hanover, USA); Dr. John Hurley (National Defense University, USA); Prof. Bill Hutchinson (Edith Cowan University, Australia); Dr. Berg Hyacinthe (State University of Haiti, Haiti); Dr. Cynthia Irvine (Naval Post Graduate School, USA); Prof. Barry Irwin (Rhodes University, South Africa); Ramkumar Jaganathan (VLB Janakiammal College of Arts and Science (affiliated to Bharathiar University), India); Russell James (Metropolitan Airports Commission, USA); Joey Jansen van Vuuren (CSIR, South Africa); Dr Chen Jim (U.S. National Defense University, USA); Dr. Andy Jones (BT, UK); James Joshi (University of Pittsburgh, USA); Prof Leonard Kabeya Mukeba Yakasham (ESURS/ISTA-KIN & ASEAD, Democratic Republic of Congo); Dr. Anthony Keane (Institute of Technology Blanchardstown, Ireland); Ayesha Khurram (National University of Sciences &Technology, Pakistan); Michael Kraft (CSC, USA); Prashant Krishnamurthy (University of Pittsburgh, USA); Mrs Marina Krotofil (Hamburg University of Technology, Germany); Dr. Dan Kuehl (National Defense University, USA); Takakazu Kurokawa (The National Defense Academy, Japan); Rauno Kuusisto (Fin-

vi

nish Defence Force, Finland); Dr. Tuija Kuusisto (National Defence University, Finland); Peter Kunz (Diamler, Germany); Arun Lakhotia (University of Louisiana Lafayertte, USA); Michael Lavine (John Hopkins University's Information Security Institute, USA); Louise Leenen (CSIR, Pretoria, South Africa); Tara Leweling (Naval Postgraduate School, Pacific Grove, USA); Dr. Andrew Liaropoulos (University of Piraeus, Greece); Dan Likarish (Regis University, Denver,, USA); Prof. Peter Likarish (Drew University, Madison, USA); Dr Sam Liles (Center for Education and Research in Information Assurance and Security (CERIAS), Purdue University, West Lafayette, Indiana, USA); Cherie Long (Georgia Gwinnett College. Lawrenceville, GA., USA); Juan Lopez Jr. (Air Force Institute of Technology, USA); Dr. Bin Lu (West Chester University of PA, USA); Volodymyr Lysenko (University of Washington, USA); Fredrick Magaya (Kampala Capital City Authority, Uganda); Dr. Bill Mahoney (University of Nebraska, Omaha, USA); Dr. hossein malekinezhad (Islamic Azad University, Iran); Dr. John McCarthy (Cranfield University , UK); Dr. Todd McDonald (Air Force Institute of Technology, USA); Dr. Jeffrey McDonald (University of South Alabama, USA); Dr. Robert Mills (Air Force Institute of Technology, USA); Dr. Nighat Mir (Effat University, Saudi Arabia); Dr. Apurva Mohan (Honeywell ACS Labs, USA); Assoc Prof Dr Salwani Mohd Daud (Universiti Teknologi Malaysia, Malaysia); Evangelos Moustakos (Middlesex University, UK); Wilmuth Mueller (Fraunhofer Institute of Optronics, System Technologies and Image Exploitation - IOSB, Germany); Dr. Srinivas Mukkamala (New Mexico Tech, Socorro, USA); Dr. Barry Mullins (Air Force Institute of Technology, USA); Dr Lilian Nassif (Public Ministry of Minas Gerais, Brazil); Muhammad Naveed (University of Engineering and Technology, Peshawar, Pakistan); Professor Abdelnaser Omran (Universiti Sains Malaysia, Malaysia); Prof. Dr. Frank Ortmeier (Otto-von-Guericke Universität, Magdeburg, Germany); Rain Ottis (Cooperative Cyber Defence Centre of Excellence, Estonia); Prof. Evgeny Pashentsev (Lomonosov Moscow State University, Russia); Dr. Gilbert Peterson (Air Force Institute of Technology, USA); Pete Peterson (The George Washington University, USA); Andy Pettigrew (George Washington University, USA); Dr. Jackie Phahlamohlaka (Council for Scientific and Industrial Research, Petoria, South Africa); Engur Pisirici (govermental - independent, Turkey); Dr. Ajeet Poonia (Govt. College Of Engineering & Technology, India); Dr. ajeet poonia (Govt. College of Engineering & Technology, India); Dr Bernardi Pranggono (Glasgow Caledonian University, UK); Prof aunshul rege (temple university, USA); Dr. Ken Revett (British University in Egypt,, Egypt); Lieutenant Colonel Ernest Robinson (U.S. Marine Corps / Air War College, USA); Dr. Neil Rowe (US Naval Postgraduate School, Monterey, USA); Daniel Ryan (National Defence University, Washington DC, USA); Julie Ryan (George Washington University, USA); Prof Julie Ryan (George Washington University, USA); Prof. Lili Saghafi (Canadian International College, Montreal, Canada); Ramanamurthy Saripalli (Pragati Engineering College, India); Sameer Saxena (IAHS Academy, Mahindra Special Services Group , India); Mark Scanlon (University College Dublin, Ireland); Dr Mark Scanlon (University College Dublin, Ireland); Corey Schou (Idaho State University, USA); Dr. Yilun Shang (Singapore University of Technology and Design, Singapore); Dr. Dan Shoemaker (Singapore University of Technology and Design, Singapore, USA); Prof. Ma Shuangge (Yale University, USA); Dr Elena Sitnikova (University of South Australia, Australia); Ass.Prof.Dr. Risby Sohaimi (National Defence University of Malaysia, Malaysia); William Sousan (University Nebraska, Omaha, USA); Dr. William Spring (University of Hertfordshire, UK); Prof. Michael Stiber (University of Washington Bothell, USA); Dr. Kevin Streff (Dakota State University, USA); Dennis Strouble (Air Force Institute of Technology, USA); Dr. arwin sumari (indonesian defense university, Indonesia); Peter Thermos (Columbia Univeristy/Palindrome Technologies, USA); Dr. Bhavani Thuraisingham (University of Texas at Dallas, USA); Mr. Patrick Tobin (University College Dublin, Ireland); Eric Trias (Air Force Institute of Technology, USA); Dr Chia-Wen Tsai (Department of Information Management, Ming Chuan University, Taiwan); Dr. Doug Twitchell (Illinois State University, USA); Dr. Shambhu Upadhyaya (University at Buffalo, USA); Renier van Heerden (CSIR, Pretoria, South Africa); Brett van Niekerk (University of KwaZulu-Natal, South Africa); Prof. Hendrik (Hein) Venter (University of Pretoria, South Africa); Prof Hendrik Venter (University of Pretoria, South Africa); Stylianos Vidalis (Newport Business School, Newport, UK); Prof. Kumar Vijaya (High Court of Andhra Pradesh, India); Dr. Natarajan Vijayarangan (Tata Consultancy Services Ltd, India); Sune Von Solms (Council for Scientific and Industrial Research, South Africa); Fahad Waseem (University of Northumbria, UK); Prof Murdoch Watney (University of Johannesburg, South Africa); Dr. Kenneth Webb (Edith Cowan University , Australia); Martha Woolson (Metropolitan Washington Airports Authority, USA); Mohamed Reda Yaich (École nationale supérieure des mines , France); Enes Yurtoglu (Turkish Air War College, Turkey); Dr Jannie Zaaiman (University of Venda, South Africa); Dr. Zehai Zhou (University of Houston-Downtown, USA); Tanya Zlateva (Boston University, USA)

A Framework of Security Safeguards for Confidentiality and Integrity of Electronic Personal Information

Prittish Dala and Hein Venter
Department of Computer Science, University of Pretoria, Pretoria, South Africa
xprittishx@gmail.com
hventer@cs.up.ac.za

Abstract: Privacy entails controlling the use and access to place, location and personal information. In South Africa, the first privacy legislation in the form of the Protection of Personal Information (POPI) Act was signed into law on 26 November 2013. The POPI Act promotes the protection of personal information by public and private institutions and specifies the minimum requirements in twelve chapters, which includes eight conditions for lawful processing of personal information. Condition Seven of the POPI Act makes specific provision for security safeguards to ensure confidentiality and integrity of personal information. However, one of the limitations of Condition Seven is that it is a requirement which is not supported by guidance relating to security safeguards to be considered to ensure confidentiality and integrity of electronic personal information. Hence, this paper aims to propose a framework based on a selection of security safeguards from several leading practices to be considered to prevent unauthorised disclosure and modification of electronic personal information stored, processed or transmitted. The authors believe that the proposed framework will facilitate the achievement and maintenance of compliance with Condition Seven of the POPI Act, with a specific focus on electronic personal information.

Keywords: protection of personal information, POPI Act, electronic personal information, security safeguards, confidentiality and integrity

1. Introduction

The currency of the digital world and oil of the Internet is personal data (Kuneva, 2009). Personal data can be bought, sold and traded creating economic value (Ali et al, 2013). Hence, the 2014 global risks identified by the World Economic Forum (2014) include data loss as a result of data fraud as a major risk within the technology domain. This is due to the advent of the information age which has presented new challenges in terms of preserving personal information (Saunders and Zucker, 1999).

According to Moore (2008), privacy entails controlling the use and access to place, location and personal information. The concept of privacy is enshrined in Section Fourteen of the South African Constitution (1996) and affords every individual a right to privacy. The Protection of Personal Information (POPI) Act (2013) defines the right to privacy as, "a right to protection against the unlawful collection, retention, dissemination and use of personal information." Personal information according to the Organisation for Economic Co-operation and Development (OECD) (2013) is regarded as any information relating to an identifiable, living and natural individual.

The value of personal information has increased significantly due to the advent of the information age (Saunders and Zucker, 1999) and this has subsequently resulted in the most prevalent crime of the new millennium known as identity theft (Hoar, 2001). This rampant form of crime largely occurs by criminals breaking into information systems of an organisation to gain access to databases, which allow them to steal personal information such as financial account numbers, addresses or identity numbers (Information Systems Audit and Control Association (ISACA), 2014).

As a result, the protection of personal information aims to protect individuals against identity theft and offers wide-ranging organisational benefits such as the protection of an organisation's brand, image and reputation, enhancing the credibility of an organisation as well as promoting consumer confidence and goodwill (Titus, 2011).

On a global scale, the OECD (2013) adopted eight privacy principles (collection, data quality, purpose specification, use limitation, security safeguards, openness, individual participation and accountability) in order to emphasize the importance of preserving privacy through data protection. These principles were used as the basis by many countries including the European Union (EU) and South Africa for developing privacy legislation with a specific focus on protecting personal information. The EU has adopted the Data Protection Directive (1995), also known as Directive 95/46/EC, to protect personal information of individuals within EU member states. The United States of America (USA) responded to meet the requirements of this directive, specifically relating to the adequacy standard, by introducing the Safe Harbor Act of 2000 designed to allow for the transfer of personal information between EU member states and the USA (Steinke, 2002). Similar to the EU, Canada has the Personal Information Protection and Electronic Document Act (PIPEDA) (2014) in place to govern how organisations collect, use and disclose personal information.

The South African response to the protection of personal information was in the form of the Protection of Personal Information (POPI) Bill first published for comment in 2005 (Stein, 2012). After undergoing numerous reviews, the POPI Bill (2009) was finally enacted and signed into law on 26 November 2013 as the Protection of Personal Information (POPI) Act (2013).

This paper focuses on Condition Seven of the POPI Act (2013), which makes provision for a selection of security safeguards to ensure confidentiality and integrity of personal information. The problem that this paper addresses is the limitation of Condition Seven of the POPI Act, which is that Condition Seven is a requirement which is not supported by guidance relating to security safeguards to be considered to ensure confidentiality and integrity of electronic personal information.

Hence, this paper aims to propose a selection security safeguards to be considered to ensure confidentiality and integrity of electronic personal information, in terms of a framework, to achieve and maintain compliance with Condition Seven of the POPI Act.

The rest of the paper is structured as follows: Section one provides a background in relation to the POPI Act. Section three highlights the requirements of Condition Seven of the POPI Act and proposes a framework that includes a selection of security safeguards to be considered for implementation to ensure confidentiality and integrity of electronic personal information. Section four provides a critical evaluation of the proposed framework. Section five concludes the paper and provides a view of future work.

2. Background

This section provides a background in relation to the protection of personal information from a South African context in the form of the Protection of Personal Information (POPI) Act (2013).

Section one of the POPI Act (2013) defines personal information as, “information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person.” The protection of personal information as promoted by the POPI Act (2013) is applicable to public and private institutions in South Africa. In order to lawfully process personal information the South African public and private institutions need to comply with the minimum requirements of the POPI Act (2013), specified in twelve chapters including eight conditions.

The “Transitional arrangements” section of the POPI Act (2013) specifies that, within one year, compliance to the Act should be achieved by public and private institutions in South Africa, unless exemptions are granted which need to be gazetted. Furthermore, the POPI Act (2013) specifies that time to comply as a result of an exemption may not exceed three years. An external Information Regulator has to be established in terms of Section Thirty Nine of the POPI Act (2013) to promote, enforce and monitor compliance to the Act. In the event that compliance is not achieved, institutions may be fined up to ten million rand, face imprisonment not exceeding ten years or receive a combination of a fine and imprisonment (POPI Act, 2013). Furthermore, institutions may suffer reputational damage, lose customers and may have to pay out millions in damages due to civil class action (Michalsons, 2014).

The next section of this paper addresses, in terms of a proposed framework, the security safeguards to be considered to ensure confidentiality and integrity of electronic personal information.

3. Proposed framework

This section provides the requirements of Condition Seven of the Protection of Personal Information (POPI) Act and proposes a framework that encapsulates the selection of security safeguards to ensure confidentiality and integrity of electronic personal information stored, processed or transmitted.

The selection of security safeguards are from several leading practices by the Information Systems Audit and Control Association (ISACA), National Institute of Standards and Technology (NIST), Office of Government Commerce United Kingdom (OGCUK) and the International Organisation for Standardisation (ISO), referred to in the rest of this paper as “leading practice organisations”. However, the proposed framework is not the implementation of leading practices such as COBIT (ISACA, 2014) RISK IT (ISACA, 2009), NIST Special Publication 800-53 (2009), ITIL (OGCUK, 2007), ISO 2230 (Drewitt, 2013) or ISO 27001 (BSI, 2005) in its entirety. The proposed framework is instead a specific selection of security safeguards prescribed by the various leading practices as a means to address a specific requirement, which in this case is to achieve compliance to Condition Seven of the POPI Act (2013).

Condition Seven of the POPI Act (2013) specifically addresses the need to implement security safeguards to ensure the confidentiality and integrity of personal information (Section Nineteen), the responsibilities for handling personal information (Section Twenty), the responsibilities of an operator processing personal information (Section Twenty One) as well as the need for notification in the event of a security compromise of personal information (Section Twenty Two).

Of significance in this study is that Section Nineteen of Condition Seven of the POPI Act is a requirement with no specific guidance in terms of how the requirement should be achieved in relation to the security safeguards to be considered to ensure the confidentiality and integrity, specifically of electronic personal information. Hence, the framework illustrated in Figure 1 below provides in four distinct phases (identify, secure, monitor and report, remediate) an approach, which includes a specific selection of security safeguards, to ultimately address the requirements of Condition Seven of the POPI Act (2013).

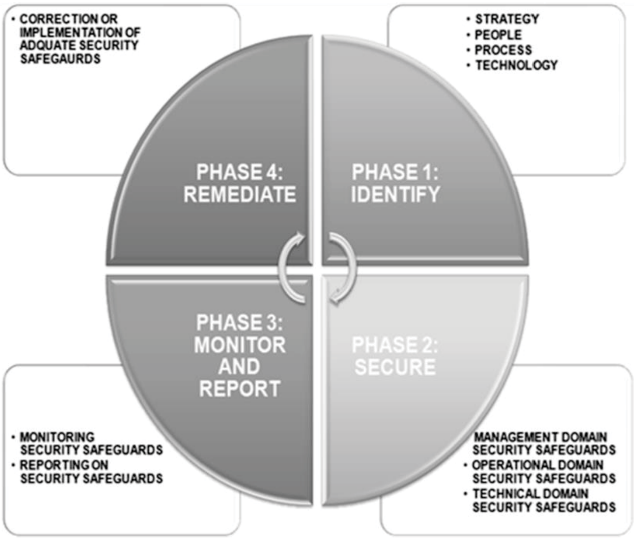

• CORRECTION OR IMPLEMENTATION OF ADQUATE SECURITY SAFEGAURDS
• STRATEGY
• PEOPLE
• PROCESS
• TECHNOLOGY
PHASE 4: REMEDIATE
PHASE 1: IDENTIFY
PHASE 3: MONITOR AND REPORT
PHASE 2: SECURE
• MONITORING SECURITY SAFEGUARDS
• REPORTING ON SECURITY SAFEGUARDS
MANAGEMENT DOMAIN SECURITY SAFEGUARDS
• OPERATIONAL DOMAIN SECURITY SAFEGUARDS
• TECHNICAL DOMAIN SECURITY SAFEGUARDS

Figure 1: Proposed framework to ensure and maintain compliance with Condition Seven of the POPI Act in relation to electronic personal information

The four phase approach leverages of the principles from the quality assurance model known as Plan-Do-Check-Act (PDCA) (British Standards Institute (BSI), 2005). This PDCA model was adopted in an information security context in terms of the ISO 27001 standard (BSI, 2005). The ISO 27001 standard (BSI, 2005) prescribes the use of the PDCA model to implement an information security management system (ISMS) as a means to effectively manage information assets of an organisation. Electronic personal information is an information asset and the four phase approach of the proposed framework for protecting electronic personal information is closely aligned to the principles of the PDCA model. Table 1, provides a description of each phase of the PDCA model and the alignment to the four phases of the proposed framework:

Table 1: Alignment between the plan-do-check-act (PDCA) model applied during the implementation of an information security management system (ISMS) and the proposed framework for protecting electronic personal information

No.	PDCA phase	Proposed framework phase
1	Plan - Establish an ISMS	Identify - Identification of electronic personal information.
2	Do - Implement and operate the ISMS	Secure - Securing the electronic personal information that needs to be protected through the selection and implementation of security safeguards.
3	Check - Monitor and review the ISMS	Monitor and Report - Monitoring and reporting to ensure that the electronic personal information remains protected and instances when the protection is not in place this should be reported in order to initiate remedial action.
4	Act - Maintain and improve the ISMS	Remediate - Remedial action taken to ensure the protection of electronic personal information is maintained.

The four phases of the proposed framework to ensure and maintain compliance with Condition Seven (Sections Nineteen, Twenty, Twenty One and Twenty Two) of the POPI Act (2013) in relation to electronic personal information, is discussed in each of the sections to follow.

Phase 1: Identify

The identification phase is based on four key perspectives: strategy, people, process and technology. The strategic perspective considers whether an organisation has identified the threats and vulnerabilities associated with the storage, processing and transmission of personal information and developed a strategy to mitigate the risk, thereby demonstrating strategic intent to comply and maintain compliance with Condition Seven of the POPI Act.

From a people perspective, this phase questions whether the relevant internal and external stakeholders have been identified who will drive the initiative to comply and maintain compliance with Condition Seven of the POPI Act.

The process perspective consists of the identification of manual and automated business processes within the organisation which store, process and transmit personal information as defined by the POPI Act (2013). Thereafter, the personal information identified should be categorised as personal information that is stored, processed and transmitted in electronic format (within information systems and their corresponding databases) as opposed to non-electronic format (hard copy or paper based outside information systems).

Lastly, the technology perspective identifies the extent to which technology may be leveraged to safeguard electronic personal information.

Phase 2: Secure

The secure phase is premised on the selection of security safeguards from several leading practices by leading practice organisations to ensure the confidentiality and integrity of electronic personal information.

The National Institute of Standards and Technology (NIST) (2009) classifies security safeguards into eighteen families which are grouped into three domains. The first domain is the management domain which focuses on managing risk by key stakeholders providing direction and intent to the protection of personal information initiative (NIST, 2009). The operational domain is the second domain, which focuses on people executing processes associated with managing and monitoring security safeguards (NIST, 2009). The third domain is the technical domain, which focuses on the implementation and execution of security safeguards driven by technology (NIST, 2009). As a result, the management, operational and technical domains form the basis of the secure phase of the proposed framework in that a selection of security safeguards as discussed in the sections below are specifically proposed for each of the three domains.

The management domain consists of the following five security safeguards:

- M1: Information security governance

This security safeguard is an integral part of governance that encompasses leadership, organisational structures as well as clear roles and responsibilities (Information Systems Audit and Control Association (ISACA), 2006) for safeguarding electronic personal information.

- M2: Risk management

The governance, evaluation and response to risks presented by electronic personal information are addressed by this security safeguard (ISACA, 2009).

- M3: Information security policy

Management direction and support for information security is achieved through a formally defined and approved information security policy (BSI, 2005).

- M4: Supplier and service level management

The supplier and service level management safeguard focuses on the contracts in place with third party operators external to the organisation and internal stakeholders within the organisation responsible for providing services in relation to electronic personal information (Office of Government Commerce United Kingdom (OGCUK), 2007).

- M5: Business continuity management

This security safeguard addresses the ability to recover from a business interruption in the most effective and efficient manner (Drewitt, 2013). This includes the recovery of electronic personal information maintained by the organisation.

The operational domain consists of the following six security safeguards:

- O1: Security procedures and processes

This security safeguard addresses the security procedures and processes in place to maintain the confidentiality and integrity of electronic personal information. The security procedure and process areas to be considered include: change and configuration management, patch management, availability management, incident management, backup management, user account and access management (OGCUK, 2007) as well as the management of encryption keys to secure data channels (BSI, 2005).

- O2: Baseline infrastructure security standards

All server, workstation and laptop operating systems, database servers, web servers, network components (firewalls, routers, wireless) that form part of the technology infrastructure to enable the protection of electronic personal information should apply baseline infrastructure security standards as a security safeguard to prevent the adoption of default configurations and to ensure consistent configurations.

- O3: Security awareness and training

Employees, contractors or third party operators need to be provided with awareness and training with regards to information security (OGCUK, 2007), with a specific focus on the security of electronic personal information.

- O4: Security monitoring, incident and reporting

All audit logs from applications as well as the technology infrastructure should be assessed in order to report on any malicious activities or data breaches of electronic personal information. Furthermore, the incident management processes may report a data breach of electronic personal information.

- O5: Security assessment

Regular security assessments should be performed to assess the security posture of the organisation from a technical, organisational, procedural, administrative or physical security perspective (Palmer et al, 2001).

- O6: Disaster recovery

People, processes and technology to ensure continued operations as well as associated with the storage, processing and transmission of electronic personal information should be defined (Drewitt, 2013).
The technical domain consists of the following nine security safeguards:

- T1: Network segmentation

The segmentation of a network entails a logical grouping of related network assets, resources and applications (Solomon, 2011). As a result, all the application and database servers that respectively process and store personal information should be located on a dedicated network segment that is separated from the rest of the corporate network.

- T2: Encrypted data channels

All electronic personal information flowing into and out of the dedicated network segment, should be encrypted and access to the data channels should be strictly monitored and controlled.

- T3: Server and network component security

All server and network components should be configured to implement the defined baseline infrastructure security standards adopted in the operational domain (O2 - Baseline infrastructure security standards).

- T4: Workstation and laptop security

Workstations and laptops should be configured to implement the defined baseline infrastructure security standards adopted and should be locked down to prevent the user to change the configuration or install additional applications not authorised by the organisation.

- T5: File integrity

All configurations associated with server and network components should be associated with a unique value known as a hash value. The hash value may be used to ascertain if unauthorised changes were affected to configurations.

- T6: Firewalls

A firewall is used to separate networks by controlling access and analysing traffic between networks (ISACA, 2013). A firewall should be used to separate the application and database servers that respectively process and store electronic personal information located on a dedicated network segment from the rest of the corporate network.

- T7: Physical and environmental security

The physical and environmental security safeguards in place within the server rooms hosting the applications as well as the technology infrastructure associated with the storage, processing and transmission of electronic personal information. Physical security safeguards to control access to the server rooms and environmental security safeguards to provide alternate power sources to ensure availability as well as to protect against environmental hazards such as floods and fire should be in place (BSI, 2005).

- T8: Centralised audit logging

Audit logs should be maintained for all applications as well as the technology infrastructure associated with storing, processing and transmitting electronic personal information. All the audit logs maintained should be sent to a centralised audit logging server where analysis may be performed to identify ineffective security safeguards as well as security incidents and to serve as the basis for conducting an investigation in the event of a data breach of electronic personal information.

- T9: Data loss prevention

The protection of data loss for data at rest, in motion or at an end point (Kanagasingham, 2008). To prevent the loss of electronic personal information specifically via workstations or laptops utilised by users to access applications processing personal information or databases storing personal information, data loss prevention should be implemented.

Phase 3: Monitor and Report

This phase is focused on monitoring and reporting. The security monitoring, incident and reporting security safeguard (O4), which forms part of the operational domain of the secure phase is critical to ensure the effectiveness of this phase. The 'monitor' aspect of this phase addresses the monitoring of security safeguards in the operational and technical domains implemented in the secure phase (phase two) of the framework to ensure that the implemented security safeguards are working as intended.

The 'report' aspect of this phase addresses the reporting of the effectiveness of the implemented security safeguards. In the event of a security compromise of electronic personal information, specific information regarding the compromise, such as the security safeguard that was circumvented and the nature and extent of personal information unlawfully obtained, may be required. Furthermore, an inspection of the audit logs maintained on the centralised audit logging server may potentially provide information of how and by whom the security compromise was performed. All information gathered relating to the security compromise, will need to be availed to internal stakeholders for further investigation as well as to the external Information Regulator to ensure compliance with Section Twenty Two (notification in the event of a security compromise of personal information) of the POPI Act (2013).

Phase 4: Remediate

During the 'monitor' aspect of phase three of the proposed framework, if it is identified that a security safeguard is not working as intended or a security compromise has occurred resulting in a circumvented security safeguard, immediate action should be taken as electronic personal information may be disclosed or modified, resulting in the compromise of electronic personal information. This compromise may negatively impact the organisation from a compliance, financial and reputational perspective. As a result, the 'remediate' phase aims to correct the current security safeguard or implement an alternate adequate security safeguard to maintain the confidentiality and integrity of electronic personal information and to ultimately ensure compliance with Section Nineteen of Condition Seven of the POPI Act (2013).

4. Critical evaluation of the proposed framework

This section provides a critical evaluation of the proposed framework in terms of benefits and limitations.

A major benefit of the proposed framework is that in four distinct phases (identify, secure, monitor and report, remediate) an approach is provided to ultimately address the requirements of Condition Seven of the POPI Act (2013) as illustrated in table 2.

Table 2: Condition seven requirements of the protection of personal information (POPI) Act addressed by the proposed framework

Condition seven section number	Condition seven requirement	Condition seven requirement addressed by the proposed framework
19	The need to implement security safeguards to ensure the confidentiality and integrity of personal information	Phase 2 - Secure Phase 4 - Remediate
20	The responsibilities for handling personal information	Phase 1 - Identify
21	The responsibilities of an operator processing personal information	Phase 1 - Identify
22	The need for notification in the event of a security compromise of personal information	Phase 3 - Monitor and Report Phase 4 - Remediate

The identify, monitor and report, and remediate phases of the proposed framework may be applied to personal information in both electronic format (within information systems and their corresponding databases) and non-electronic format (hard copy or paper based outside information systems). In addition, the security safeguards in the management and operational domains of the secure phase may be applied to personal information in both electronic and non-electronic format. Most importantly, twenty security safeguards are identified as part of the secure phase (consisting of three domains - management, operational and technical) of the proposed framework, which may be considered in order to ultimately ensure confidentiality and integrity of electronic personal information.

Table 3 below provides a summary of the source of the twenty selected safeguards in terms of leading practices to ensure confidentiality and integrity of electronic personal information and serves as a point of reference for detailed guidance relating to the proposed safeguards. For example, when addressing the the disaster recovery security safeguard (O6 in table 3), ISO 22301 and ISO 27001 as well as the NIST Special Publication 800-53 leading practices may provide the required guidance.

Table 3: Source of the selected safeguards to specifically ensure confidentiality and integrity of electronic personal information as required by condition seven of the Popi Act

Selected Safeguard	ISACA	NIST	OGCUK	ISO
Management Domain				
M1: Information security governance	COBIT			ISO 27001
M2: Risk management	COBIT RISK IT			
M3: Information security policy				ISO 27001
M4: Supplier and service level management	COBIT		ITIL	
M5: Business continuity management	COBIT			ISO 22301 ISO 27001
Operational Domain				
O1: Security procedures and processes	COBIT		ITIL	ISO 27001
O2: Baseline infrastructure security standards		NIST Special Publication 800-53		
O3: Security awareness and training		NIST Special Publication 800-53	ITIL	ISO 27001
O4: Security monitoring, incident and reporting	COBIT	NIST Special Publication 800-53	ITIL	
O5: Security assessment		NIST Special Publication 800-53		
O6: Disaster recovery		NIST Special Publication 800-53		ISO 22301 ISO 27001
Technical Domain				
T1: Network segmentation		NIST Special Publication 800-53		
T2: Encrypted data channels		NIST Special Publication 800-53		ISO 27001
T3: Server and network component security	COBIT	NIST Special Publication 800-53		
T4: Workstation and laptop security	COBIT	NIST Special Publication 800-53		
T5: File integrity	COBIT		ITIL	
T6: Firewalls		NIST Special Publication 800-53		
T7: Physical and environmental security	COBIT	NIST Special Publication 800-53		ISO 27001
T8: Centralised audit logging	COBIT	NIST Special Publication 800-53		ISO 27001
T9: Data loss prevention	COBIT	NIST Special Publication 800-53		ISO 22301

A limitation of the proposed framework is that the security safeguards in the technical domain of the secure phase is focused on the personal information stored, processed and transmitted in electronic format as opposed to non-electronic format. In addition, the proposed framework is not the implementation of leading practices such as COBIT (ISACA, 2014) RISK IT (ISACA, 2009), NIST Special Publication 800-53 (2009), ITIL (OGCUK, 2007), ISO 2230 (Drewitt, 2013) or ISO 27001 (BSI, 2005) in its entirety. However, the proposed framework is instead a specific selection of security safeguards prescribed by the various leading practices as a means to address a specific requirement, which in this case is to achieve compliance to Condition Seven of the POPI Act (2013). Furthermore, the proposed framework is limited to addressing only the requirements of Condition Seven of the POPI Act (2013) in relation to electronic personal information.

5. Conclusion and future work

In this paper, the Protection of Personal Information (POPI) Act was explored with specific emphasis on Condition Seven of the POPI Act (2013), which makes provision for security safeguards to ensure confidentiality and integrity of personal information. However, the challenge identified is that Condition Seven of the POPI Act is a requirement with no specific information in terms of how the requirement should be achieved, with a specific focus on electronic personal information. As a result, the proposed framework outlined a selection of security safeguards that should be considered in a four phase approach (identify, secure, monitor and report, and remediate) to ultimately achieve and maintain compliance with Condition Seven of the POPI Act.

In terms of future work, a model of operation will be proposed that aims to provide a holistic approach consisting of twenty security safeguards across three domains (management, operational and technical) to be considered for implementation to ensure confidentiality and integrity of electronic personal information as required by Condition Seven of the POPI Act. Furthermore, a rigorous comparison of the requirements to protect personal information will be conducted between the POPI Act and the Data Protection Directive adopted by the European Union based on the privacy principles adopted by the Organisation for Economic Co-operation and Development (OECD).

References

Ali, A., Eggers, W.D., Hamill, R. and Hersey, J. (2013) (2013) “Data as the New Currency - Government’s Role in Facilitating the Exchange”, *Deloitte Review*, Issue 13, p.19.

British Standards Institute (BSI). (2005) “BS ISO/IEC 27001:2005: Information Technology - Security Techniques - Information Security Management Systems - Requirements”, First Edition, p.VI and pp.1-33.

Drewitt, T. (2013) “A Manager’s Guide to ISO22301”, *IT Governance Publishing*, pp.11-18 and pp.100-112.

European Parliament. (1995) “Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data”, *Official Journal of the European Communities*, Vol.38, pp.31-50.

Government of Canada. (2014) “Personal Information Protection and Electronic Document Act (PIPEDA)”, pp.1-47.

Hoar, S.B. (2001) “Identity Theft: The Crime of the New Millennium”, *Oregon Law Review*, Vol.80, No. 4, p. 1423.

Information Systems Audit and Control Association (ISACA) (2006) “Information Security Governance: Guidance for Boards of Directors and Executive”, Second Edition, pp.7-45.

Information Systems Audit and Control Association (ISACA) (2009) “The Risk IT Framework”, pp.17-30.

Information Systems Audit and Control Association (ISACA). (2013) “CISA Review Manual 2013”, p.341.

Information Systems Audit and Control Association (ISACA). (2014) “Risk to Entities Regarding Data Breaches - Lessons from a Brief Case Study”, Information Systems Audit and Control Association (ISACA) Journal, Vol.2, p.14.

Information Systems Audit and Control Association (ISACA). (2014) “COBIT 5”, pp.11-88.

Kanagasingham, P. (2008) “Data Loss Prevention”, *SANS Institute*, p.5, [online], https://www.sans.org/reading-room/whitepapers/dlp/data-loss-prevention-32883.

Kuneva, M. (2009) “Keynote Speech - Roundtable on Online Data Collection, Targeting and Profiling”, *European Comission*, p.2, [online], http://europa.eu/rapid/press-release_SPEECH-09-156_en.pdf.

Michalsons. (2014) “Protection of Personal Information Act - POPI”, [online], http://www.michalsons.co.za/protection-of-personal-information-act-popi/11105.

Moore. A.D. (2008) “Defining Privacy”, *Journal of Social Philosophy*, Vol.39, No.3, p.425.

National Institute of Standards and Technology (NIST). (2009) “Recommended Security Controls for Federal Information Systems and Organisations”, *NIST Special Publication 800-53*, Revision 3, pp.1-238.

Office of Government Commerce United Kingdom (OGCUK). (2007) “ITIL - Service Design”, pp.65-78 and pp.149-164.

Office of Government Commerce United Kingdom (OGCUK). (2007) “The Official Introduction to the ITIL Service Lifecycle”, pp.55-124.

Organisation for Economic Co-operation and Development (OECD). (2013) “OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data”, [online], http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf.

Palmer, M.E., Patilla, J.C., Moser, E.P. and Robinson, C. (2001) “Information Security Policy Framework: Best Practices for Security Policy in the E-commerce Age”, *Information Systems Security*, Vol.10, Issue 2, p.11.

Republic of South Africa. (1996) “Constitution of the Republic of South Africa (Act 108 of 1996)”, Pretoria: Government Printer, Issue 32, p.1249.

Republic of South Africa. (2009) "Protection of Personal Information (POPI) Bill", Cape Town and Pretoria: Government Printer, pp.1-50.

Republic of South Africa (2013) "Protection of Personal Information (POPI) Act (Act 4 of 2013)", Cape Town: Government Printer, No.37067, pp.2-146.

Saunders, K.M. and Zucker, B. (1999) "Counteracting Identity Fraud in the Information Age: The Identity Theft and Assumption Deterrence Act", *International Review of Law, Computers & Technology*, Vol.13, No. 2, p.183.

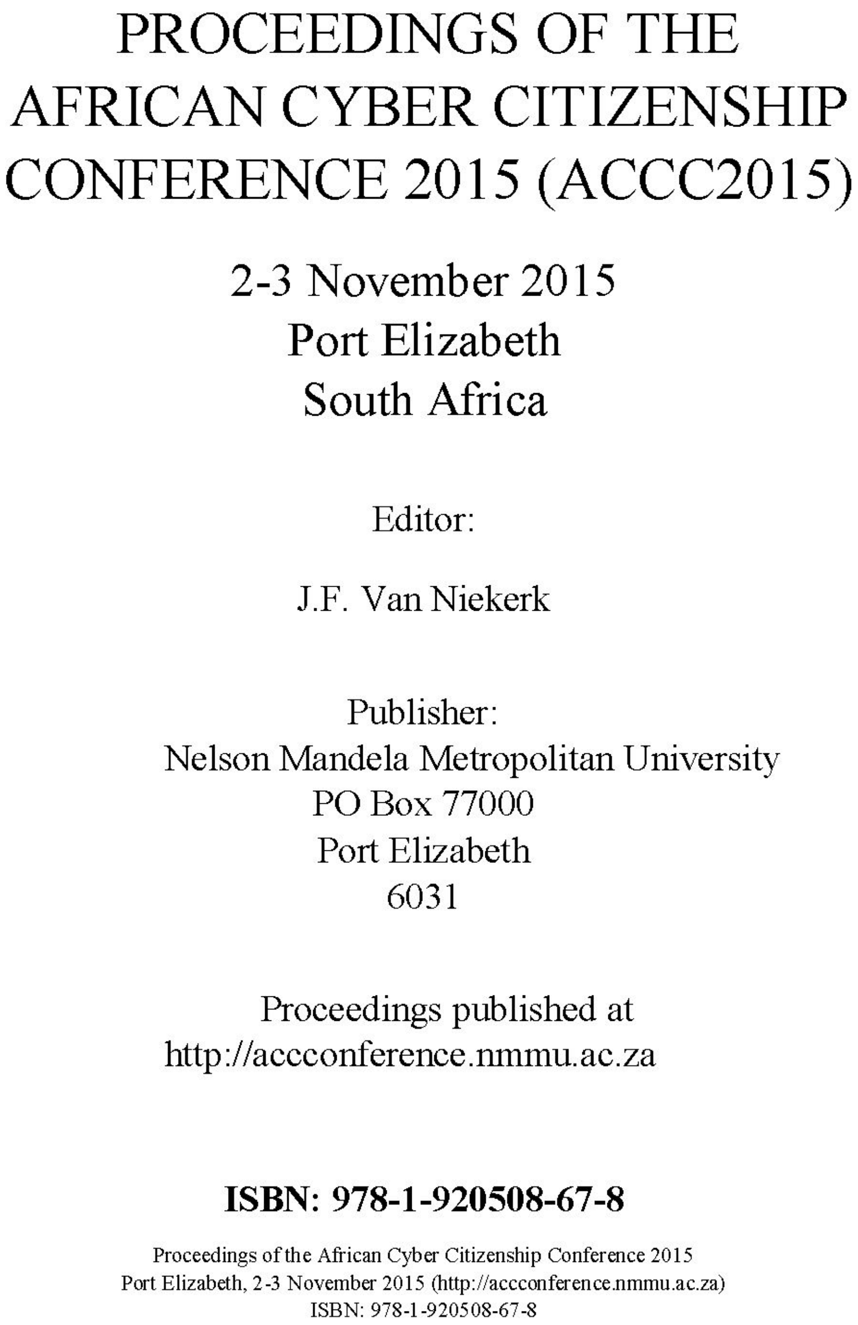
Solomon, M. (2011) "Using Network Segmentation to Protect the Modern Enterprise Network", *Security Week*, [online], http://www.securityweek.com/using-network-segmentation-protect-modern-enterprise-network.

Stein, P. (2012) "South Africa's EU-style Data Protection Law", *Without Prejudice*, Vol.12, Issue 10, pp.48-49.

Steinke, G. (2002) "Data Privacy Approaches from US and EU Perspectives", Telematics and Informatics, Vol.19, pp.193-200.

Titus. (2011) "Protecting Personally Identifiable Information (PII) with Classification and Content Inspection", *Titus White Paper*, p.5, [online], http://www.titus.com/resources/marketo/WEB_COM_WP_Protecting_PII.pdf.

World Economic Forum (WEF). (2014) "Global Risks 2014", *Insight Report*, 9th Edition, pp.12-13, [online], http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2014.pdf.



PROCEEDINGS OF THE AFRICAN CYBER CITIZENSHIP CONFERENCE 2015 (ACCC2015)

2-3 November 2015
Port Elizabeth
South Africa

Editor:

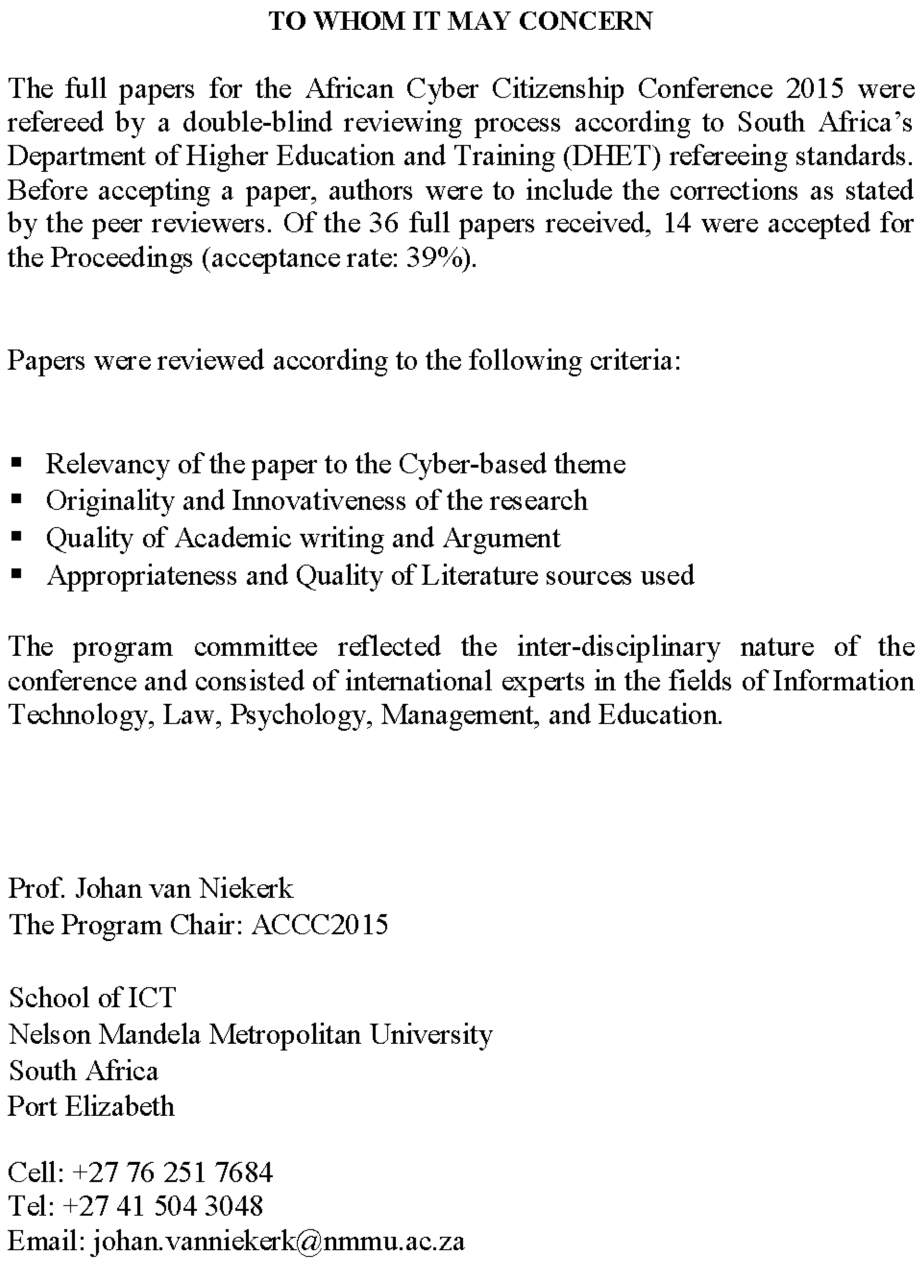
J.F. Van Niekerk

Publisher:
Nelson Mandela Metropolitan University
PO Box 77000
Port Elizabeth
6031

Proceedings published at
http://accconference.nmmu.ac.za

ISBN: 978-1-920508-67-8

Proceedings of the African Cyber Citizenship Conference 2015
Port Elizabeth, 2-3 November 2015 (http://accconference.nmmu.ac.za)
ISBN: 978-1-920508-67-8



TO WHOM IT MAY CONCERN

The full papers for the African Cyber Citizenship Conference 2015 were refereed by a double-blind reviewing process according to South Africa's Department of Higher Education and Training (DHET) refereeing standards. Before accepting a paper, authors were to include the corrections as stated by the peer reviewers. Of the 36 full papers received, 14 were accepted for the Proceedings (acceptance rate: 39%).

Papers were reviewed according to the following criteria:

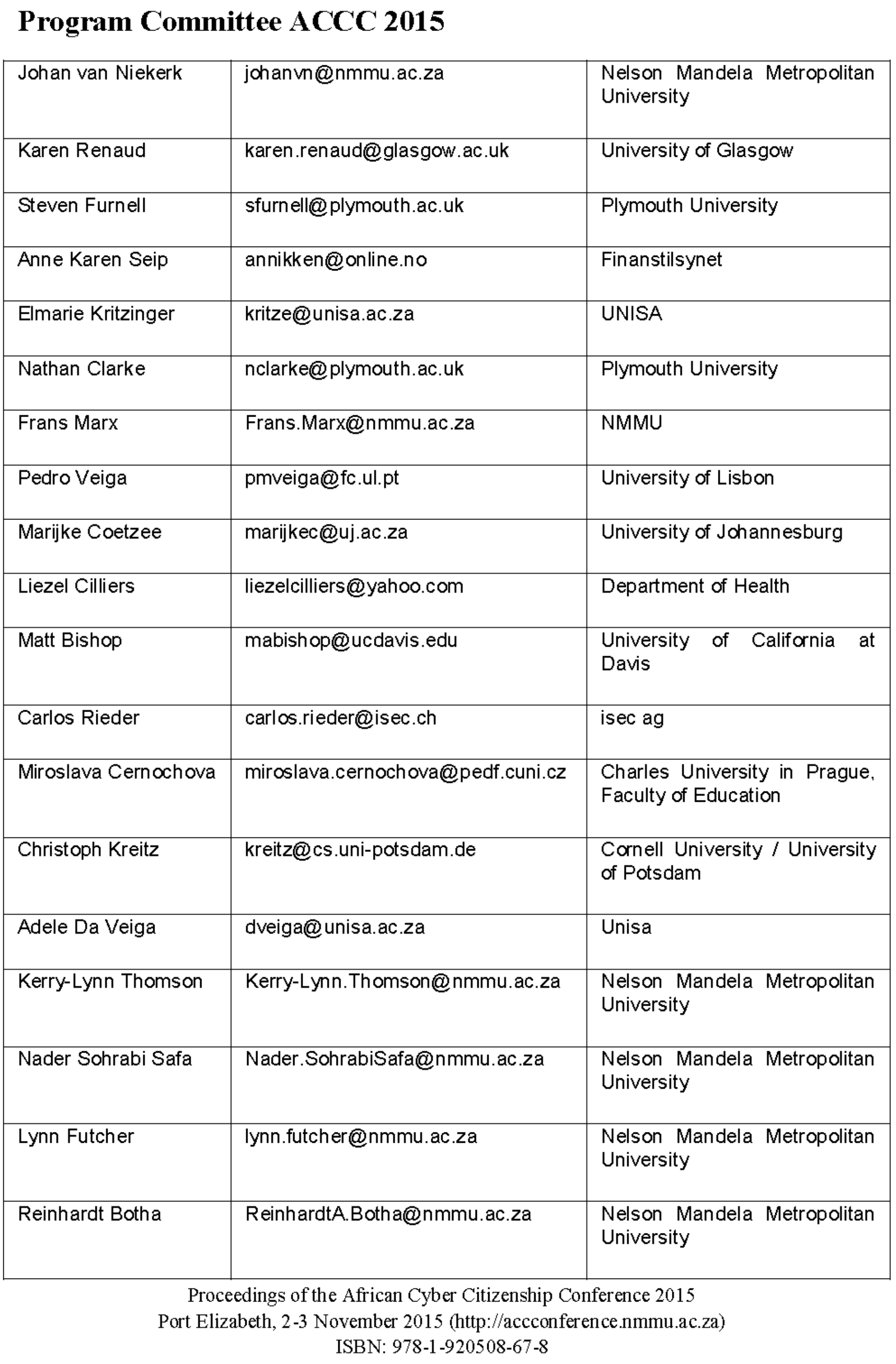
- Relevancy of the paper to the Cyber-based theme
- Originality and Innovativeness of the research
- Quality of Academic writing and Argument
- Appropriateness and Quality of Literature sources used

The program committee reflected the inter-disciplinary nature of the conference and consisted of international experts in the fields of Information Technology, Law, Psychology, Management, and Education.

Prof. Johan van Niekerk
The Program Chair: ACCC2015

School of ICT
Nelson Mandela Metropolitan University
South Africa
Port Elizabeth

Cell: +27 76 251 7684
Tel: +27 41 504 3048
Email: johan.vanniekerk@nmmu.ac.za



Program Committee ACCC 2015

Johan van Niekerk	johanvn@nmmu.ac.za	Nelson Mandela Metropolitan University
Karen Renaud	karen.renaud@glasgow.ac.uk	University of Glasgow
Steven Furnell	sfurnell@plymouth.ac.uk	Plymouth University
Anne Karen Seip	annikken@online.no	Finanstilsynet
Elmarie Kritzinger	kritze@unisa.ac.za	UNISA
Nathan Clarke	nclarke@plymouth.ac.uk	Plymouth University
Frans Marx	Frans.Marx@nmmu.ac.za	NMMU
Pedro Veiga	pmveiga@fc.ul.pt	University of Lisbon
Marijke Coetzee	marijkec@uj.ac.za	University of Johannesburg
Liezel Cilliers	liezelcilliers@yahoo.com	Department of Health
Matt Bishop	mabishop@ucdavis.edu	University of California at Davis
Carlos Rieder	carlos.rieder@isec.ch	isec ag
Miroslava Cernochova	miroslava.cernochova@pedf.cuni.cz	Charles University in Prague, Faculty of Education
Christoph Kreitz	kreitz@cs.uni-potsdam.de	Cornell University / University of Potsdam
Adele Da Veiga	dveiga@unisa.ac.za	Unisa
Kerry-Lynn Thomson	Kerry-Lynn.Thomson@nmmu.ac.za	Nelson Mandela Metropolitan University
Nader Sohrabi Safa	Nader.SohrabiSafa@nmmu.ac.za	Nelson Mandela Metropolitan University
Lynn Futcher	lynn.futcher@nmmu.ac.za	Nelson Mandela Metropolitan University
Reinhardt Botha	ReinhardtA.Botha@nmmu.ac.za	Nelson Mandela Metropolitan University

The Extent to which Privacy Legislation of the European Union and South Africa Addresses the 2013 OECD Guidelines

P.Dala and H.S.Venter
Department of Computer Science, University of Pretoria, Pretoria, South Africa
e-mail: xprittishx@gmail.com and hventer@cs.up.ac.za

Abstract

Privacy entails controlling the use and access to place, location and personal information. The value of personal information has increased significantly due to the advent of the information age and with it, the occurrence of the most prevalent crime of the new millennium known as "identity theft". Largely as a response to ever increasing use of personal information, the Organisation for Economic Co-operation and Development (OECD) adopted guidelines on trans-border data flows and the protection of privacy. These guidelines included eight privacy principles (collection, data quality, purpose specification, use limitation, security safeguards, openness, individual participation and accountability) to govern the preservation of privacy and trans-border flow of personal data. The European Union adopted the Data Protection Directive (also known as Directive 95/46/EC) of 1995 to protect the personal information of individuals within European Union member states. In South Africa, privacy legislation in the form of the Protection of Personal Information (POPI) Act was signed into law on 26 November 2013. The POPI Act promotes the protection of personal information by public and private institutions and specifies the minimum requirements which include eight conditions for lawful processing of personal information. To date, an analysis to ascertain the extent to which the European Union and South African privacy legislation addresses the 2013 OECD guidelines on trans-border data flows and the protection of privacy including the eight privacy principles, has not been undertaken. Hence, this paper aims to initiate such an analysis, with particular focus on the extent to which the European Union's Data Protection Directive and the South African POPI Act addresses the 2013 OECD guidelines on trans-border data flows and the protection of privacy, including the eight privacy principles. In addition, similarities and differences were identified between the Data Protection Directive (1995) and the POPI Act (2013) as a result of the analysis.

Keywords

Protection of personal information, POPI Act, Data protection directive, OECD privacy principles

Proceedings of the African Cyber Citizenship Conference 2015
Port Elizabeth, 2-3 November 2015 (http://accconference.nmmu.ac.za)
ISBN: 978-1-920508-67-8

1. Introduction

The currency of the digital world and oil of the Internet is personal data (Kuneva, 2009). Personal data can be bought, sold and traded creating economic value (Ali et al. 2013). Hence, global risks identified by the World Economic Forum (2014) include data loss as a result of data fraud as a major risk within the technology domain. This is due to the advent of the information age which has presented new challenges in terms of preserving personal information (Saunders and Zucker, 1999).

Privacy entails controlling the use and access to place, location and personal information (Moore, 2008). The value of personal information has increased significantly due to the advent of the information age (Saunders and Zucker, 1999) and this has subsequently resulted in the most prevalent crime of the new millennium known as identity theft (Hoar, 2001). This rampant form of crime according to the Information Systems Audit and Control Association (ISACA) (2014) largely occurs when criminals electronically break into information systems (such as those owned by organisations) to gain access to databases, which allows them to steal personal information such as financial account numbers, addresses or identity numbers.

As a result, the protection of personal information aims to protect individuals against identity theft and offers wide-ranging organisational benefits such as the protection of an organisation's brand, image and reputation, enhancing the credibility of an organisation as well as promoting consumer confidence and goodwill (Titus, 2011).

The Organisation for Economic Co-operation and Development (OECD) (1980 and 2013) adopted guidelines on trans-border data flows and the protection of privacy. The guidelines included eight privacy principles (collection, data quality, purpose specification, use limitation, security safeguards, openness, individual participation and accountability) to govern the preservation of privacy and trans-border flow of personal data.

Privacy legislation in the European Union took the form of the Data Protection Directive (also known as Directive 95/46/EC) of 1995, which aimed to protect the personal information of individuals within European Union member states.

The South African privacy legislation response to protect personal information was in the form of the Protection of Personal Information (POPI) Bill first published for comment in 2005 (Stein, 2012). After undergoing numerous reviews, the POPI Bill (2009) was finally enacted and signed into law on 26 November 2013 as the Protection of Personal Information (POPI) Act (2013).

The extent to which the European Union and South African privacy legislation addresses the 2013 OECD guidelines on trans-border data flows and the protection of privacy, which includes the eight privacy principles, has not been explored. Hence, this paper aims to analyse the extent to which the European Union Data Protection Directive and the South African POPI Act addresses the 2013 OECD guidelines on trans-border data flows and the protection of privacy, which includes the eight privacy principles. Thus, the contribution of this paper is to provide a comparison of specific privacy legislation in relation to the 2013 OECD guidelines, instead of comparing privacy legislation of specific countries or regions to each other, which has been conducted by several researchers such as Botha et al. (2015) and Dowling (2009).

This paper is one of a series of papers that aim to provide an understanding of the POPI Act as well as:

a framework of security safeguards for confidentiality and integrity of electronic personal information as required by Condition Seven of the POPI Act, which has been completed and submitted.

the extent to which the European Union and South African privacy legislation addresses the 2013 OECD guidelines on trans-border data flows and the protection of privacy, including eight privacy principles, which is this paper.

the current state of security safeguards within South African institutions, in relation to electronic personal information, to achieve compliance to Condition Seven of the POPI Act, which is a forthcoming paper; and

a model of operation to guide the implementation of the security safeguards, as required by Condition Seven of the POPI Act, which is a forthcoming paper.

The paper is structured as follows: Section 2 provides a background of the OECD guidelines on trans-border data flows and the protection of privacy as well as the European Union and South African privacy legislation. Section 3 analyses the extent to which the European Union Data Protection Directive and the South African POPI Act addresses the 2013 OECD guidelines on trans-border data flows and the protection of privacy, which includes the eight privacy principles. Section 4 provides a critical evaluation of the analysis. Section 5 concludes the paper and also presents future work.

2. Background

This section provides a background of the Organisation for Economic Co-operation and Development (OECD) guidelines on trans-border data flows and the protection of privacy as well as the European Union and South African privacy legislation.

OECD Guidelines on Trans-Border Data Flows and the Protection of Privacy

In 1980, the OECD adopted guidelines on trans-border data flows and the protection of privacy. At that stage, the major drivers for these guidelines were the threats associated with privacy due to the ever increasing use of personal information and the impact restrictions on the flow of information will have on the global economy (OECD, 2011). As a result, the guidelines included eight privacy principles (collection, data quality, purpose specification, use limitation, security safeguards, openness, individual participation and accountability) to govern the preservation of privacy and trans-border flow of personal data (OECD, 1980). These guidelines were recommended to OECD member states to be applied to all personal data by both public and private institutions [OECD, 1980 and Kirby, 2011).

The guidelines on trans-border data flows and the protection of privacy were revised by the OECD in 2013. Major drivers for the revision of the guidelines according to Kuner (2011), was due to increased globalisation of the world economy, growing economic importance of data processing, ubiquity of data transfers over the Internet, greater direct involvement in trans-border data flows, the changing role of geography and the growing risk to the privacy of individuals.

The eight privacy principles prescribed within the guidelines by the OECD in 1980 remained unchanged in the 2013 revision (Kuschewsky, 2014). However, the revised guidelines by OECD (2013) placed greater focus on implementing accountability, the basic principles of international application in terms of free flow and legitimate restrictions, national implementation as well as international co-operation and interoperability.

European Union Data Protection Directive

Privacy legislation in the European Union takes the form of the Data Protection Directive (also known as Directive 95/46/EC) of 1995.

The purpose of the Data Protection Directive (1995) as outlined in article 1 is to ensure that, “member states shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data”. In addition, the free flow of personal data between member states is encouraged as long as privacy is preserved.

Article 2 of the Data Protection Directive of 1995 defines personal data as, “any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity".

The protection of personal data as promoted by the Data Protection Directive (1995) is applicable to European Union member states. However, each European Union member state enacts their own privacy laws based on the Data Protection Directive (1995) which consists of 34 articles within 7 chapters.

The Data Protection Directive (1995) is not a regulation and this has allowed European Union member states to inconsistently interpret and apply the Directive within their own enacted privacy legislation (Lynch, 2013). For example, chapter 3 of the Directive makes provision for judicial remedies, liability and sanctions, however the conditions, actual penalties and enforcement in the event of a breach of personal information differs for each European Union member state.

As a result, in 2012 the European Commission proposed that the Data Protection Directive (1995) be replaced by the General Data Protection Regulation (2012). This proposal marked a paradigm shift from "directive" to "regulation" that sought to provide a single data protection law applicable to all European Union member states, thus preventing the need for individual privacy legislation by each European Union member state. According to Greens (2015), it is envisaged that the General Data Protection Regulation will be adopted by the end of 2015 and will be followed by a two year transition period to allow European Union member states to comply, followed by enforcement of the regulation.

South African Protection of Personal Information Act

South African privacy legislation took the form of the Protection of Personal Information (POPI) Bill, first published for comment in 2005 (Stein, 2012). After undergoing numerous reviews, the POPI Bill was finally enacted and signed into law on 26 November 2013 as the Protection of Personal Information (POPI) Act, with the purpose clearly outlined within section 2 (2013).

Section 1 of the POPI Act (2013) defines personal information as, "information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person."

The protection of personal information as promoted by the POPI Act (2013) is applicable to public and private institutions in South Africa. In order to lawfully process personal information the South African public and private institutions need to comply with the minimum requirements of the POPI Act (2013), specified within 12 chapters including 8 conditions.

Although the POPI Act was signed into law on 26 November 2013 the enforcement date of POPI Act is still to be announced. However, the “Transitional arrangements” section of the POPI Act (2013) contained in chapter 11 specifies that within 1 year, compliance to the Act should be achieved by public and private institutions in South Africa, unless exemptions which are gazetted are granted. In the event of such exemption, however, the time granted to comply may not exceed 3 years.

An external Information Regulator has to be established in terms of section 39 of the POPI Act (2013) to promote, enforce and monitor compliance to the POPI Act. According to Michalsons (2014), in the event that compliance to the POPI Act is not achieved, members of the South African public and private institutions may be fined up to 10 million rand, face imprisonment not exceeding 10 years or receive a combination of a fine and imprisonment. Furthermore, institutions may suffer reputational damage, lose customers and may have to pay out millions in damages due to civil class action (Michalsons, 2014).

3. Analysis of the European Union and South African privacy legislation in relation to the 2013 OECD guidelines

This section analyses the extent to which the European Union Data Protection Directive (1995) and the South African Protection of Personal Information (POPI) Act (2013) address the 2013 Organisation for Economic Co-operation and Development (OECD) guidelines on trans-border data flows and the protection of privacy.

The analysis uses the eight privacy principles (collection, data quality, purpose specification, use limitation, security safeguards, openness, individual participation and accountability) as well as the additional focus areas (implementing accountability, basic principles of international application in terms of free flow and legitimate restrictions, national implementation and international co-operation and interoperability) of the 2013 OECD guidelines on trans-border data flows and the protection of privacy, as the basis for comparison. The analysis is reflected in table 1 below, which provides the extent to which the European Union Data Protection Directive (1995) and South African POPI Act (2013) addresses the 2013 OECD guidelines.

No.	Description of the 2013 OECD guideline on trans-border data flows and the protection of privacy	Requirement addressed by the European Union Data Protection Directive of 1995	Requirement addressed by the South African Protection of Personal Information Act

No.	Description of the 2013 OECD guideline on trans-border data flows and the protection of privacy	Requirement addressed by the European Union Data Protection Directive of 1995	Requirement addressed by the South African Protection of Personal Information Act
1	Collection limitation principle	Yes - Chapter 2: General rules on the lawfulness of the processing of personal data (Articles 5 and 6).	Yes - Chapter 3: Conditions for lawful processing of personal information (Conditions 2, 3 and 4).
2	Data quality principle	Yes - Chapter 2: General rules on the lawfulness of the processing of personal data (Article 6).	Yes - Chapter 3: Conditions for lawful processing of personal information (Condition 5).
3	Purpose specification principle	Yes - Chapter 2: General rules on the lawfulness of the processing of personal data (Articles 6, 7, 8, 9, 10 and 11).	Yes - Chapter 3: Conditions for lawful processing of personal information (Conditions 3 and 4).
4	Use limitation principle	Yes - Chapter 2: General rules on the lawfulness of the processing of personal data (Articles 6, 7, 8, 9, 10, 11, 20 and 21).	Yes - Chapter 3: Conditions for lawful processing of personal information (Conditions 2, 3 and 4) and Chapter 6: Prior authorisation.
5	Security safeguards principle	Yes - Chapter 2: General rules on the lawfulness of the processing of personal data (Articles 16 and 17).	Yes - Chapter 3: Conditions for lawful processing of personal information (Condition 7).
6	Openness principle	Yes - Chapter 2: General rules on the lawfulness of the processing of personal data (Articles 12 and 13).	Yes - Chapter 3: Conditions for lawful processing of personal information (Condition 6).
7	Individual participation principle	Yes - Chapter 2: General rules on the lawfulness of the processing of personal data (Articles 14 and 15).	Yes - Chapter 3: Conditions for lawful processing of personal information (Condition 8).
8	Accountability	Yes - Chapter 1: General provisions (Article 4) and	Yes - Chapter 3: Conditions for lawful processing of

No.	Description of the 2013 OECD guideline on trans-border data flows and the protection of privacy	Requirement addressed by the European Union Data Protection Directive of 1995	Requirement addressed by the South African Protection of Personal Information Act
	principle	Chapter 2: General rules on the lawfulness of the processing of personal data (Article 6).	personal information (Condition 1).
9	Implementing accountability: Privacy management programme	No - Specific reference is not made to a privacy management programme.	No - Specific reference is not made to a privacy management programme. However, chapter 11 makes reference to an administrative fine being enforced in the event of failure to conduct a risk assessment and maintain good policies, procedures and practices to protect personal information.
10	Implementing accountability: Privacy enforcement authorities	Yes - Chapter 6: Supervisory authority and working party on the protection of individuals with regard to the processing of personal data (Article 28).	Yes - Chapter 5: Information regulator.
11	Implementing accountability: Data security breach notification	Yes - Chapter 2: General rules on the lawfulness of the processing of personal data (Article 18).	Yes - Chapter 3: Conditions for lawful processing of personal information (Condition 7).
12	Basic principles of international application in terms of free flow and legitimate restrictions: Trans-border flows of personal data	Yes - Chapter 4: Transfer of personal data to third countries (Articles 25 and 26).	Yes - Chapter 9: Trans-border information flows.
13	National implementation	No - The European Union Data Protection Directive is not a regulation, it is a directive. As a result, Chapter 1: Article 4 states	Yes - The Protection of Personal Information Act is applicable to all public and private institutions in South Africa. At this stage the Act

No.	Description of the 2013 OECD guideline on trans-border data flows and the protection of privacy	Requirement addressed by the European Union Data Protection Directive of 1995	Requirement addressed by the South African Protection of Personal Information Act
		that each member state shall apply the national provisions it adopts pursuant to the directive.	was signed into law on 26 November 2013. The enforcement date for the POPI Act is still to be announced. Thereafter, a one year transition period will apply to allow all public and private institutions in South Africa to comply with the POPI Act, after which enforcement will be monitored by the Information Regulator.
14	International co-operation and interoperability	Yes - Chapter 4: Transfer of personal data to third countries (Articles 25 and 26).	Yes - Chapter 5: Information regulator (co-operating on a national and international basis with other persons and bodies concerned with the protection of personal information).

Table 1: Extent to which the European Union Data Protection Directive (1995) and the South African Protection of Personal Information Act (2013) addresses the 2013 OECD guidelines (2013)

4. Critical evaluation of the analysis of the European Union and South African privacy legislation in relation to the 2013 OECD guidelines

This section provides a critical evaluation of the analysis performed in section three of this paper, to ascertain the extent to which the European Union Data Protection Directive (1995) and the South African Protection of Personal Information (POPI) Act (2013) addresses the 2013 Organisation for Economic Co-operation and Development (OECD) guidelines on trans-border data flows and the protection of privacy, which includes eight privacy principles.

The European Union Data Protection Directive (1995) addresses the eight privacy principles (collection, data quality, purpose specification, use limitation, security safeguards, openness, individual participation and accountability) from the 2013 OECD guidelines on trans-border data flows and the protection of privacy. However, the Directive does not make reference to a privacy management programme. In terms of implementing accountability an adequate privacy management programme has to be defined and implemented and be subject to review from a privacy enforcement authority. The programme includes providing notice to the privacy enforcement authority in the event of a breach of personal data. In addition, the Directive does not address the national implementation requirement as it is not a regulation but a directive.

In terms of the South African POPI Act (2013), the 2013 OECD guidelines on trans-border data flows and the protection of privacy, including the eight privacy principles are addressed. The only exception is that no specific reference is made to a privacy management programme within the POPI Act. However, the POPI Act does make reference to an administrative fine being enforced in the event of failure to conduct a risk assessment and maintain good policies, procedures and practices to protect personal information. Furthermore, a privacy enforcement authority in the form of the Information Regulator is required by the POPI Act to monitor enforcement and receive notifications relating to breaches of personal data.

Furthermore, similarities and differences were noted between the Data Protection Directive (1995) and the POPI Act (2013) as a result of the analysis performed in section three of this paper. Firstly, all eight privacy principles specified by the OECD (2013) are addressed by both the Data Protection Directive (1995) and POPI Act (2013). Secondly, the Data Protection Directive (1995) and POPI Act (2013) both do not make provision for a privacy management programme. The major difference between the Data Protection Directive (1995) and the POPI Act (2013) is that the POPI Act is enforceable compared to the Data Protection Directive which is not enforceable. The Data Protection Directive (1995) is not enforceable as it is not a regulation, but is viewed as a guideline to serve as a frame of reference for European

Union member states when developing their own privacy legislation, which becomes enforceable within that member state once enacted.

5. Conclusion and future work

In this paper the 2013 Organisation for Economic Co-operation and Development (OECD) guidelines on trans-border data flows and the protection of privacy, which includes eight privacy principles as well as the European Union Data Protection Directive (1995) and the South African Protection of Personal Information (POPI) Act (2013) were explored.

This gave rise to an analysis of the European Union and South African privacy legislation in relation to the 2013 OECD guidelines. The analysis was followed by a critical evaluation that identified the extent to which the Data Protection Directive (1995) and the POPI Act (2013) address the 2013 OECD guidelines on trans-border data flows and the protection of privacy. In addition, the critical evaluation identified similarities and differences between the Data Protection Directive (1995) and the POPI Act (2013).

In terms of future work, the current state of security safeguards within South African institutions, in relation to electronic personal information, to achieve compliance to Condition Seven of the POPI Act (2013) will be explored. In addition, a model of operation will be proposed to guide the implementation of the security safeguards to ensure confidentiality and integrity of electronic personal information stored, processed and transmitted, as required by Condition Seven of the POPI Act (2013).

6. References

Ali, A., Eggers, W.D., Hamill, R. and Hersey, J. (2013), “Data as the New Currency - Government’s Role in Facilitating the Exchange”, Deloitte Review, Issue 13, p.19.

Botha, J., Eloff, M.M. and Swart, I. (2015), “Evaluation of Online Resources on the Implementation of the Protection of Personal Information Act in South Africa”, Proceedings of the 10th International Conference on Cyber Warfare and Security, Kruger National Park, South Africa, 24-25 March 2015, p.41.

Dowling Jr, D.C. (2009), "International Data Protection and Privacy Law", White Case, pp.2-33, http://www.whitecase.com/files/publication/367982f8-6dc9-478e-ab2f-5fdf2d96f84a/presentation/publicationattachment/30c48c85-a6c4-4c37-84bd-6a4851f87a77/article_intldataprotectionandprivacylaw_v5.pdf, (Accessed 27 June 2015).

European Parliament. (1995), "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data", Official Journal of the European Communities, Vol.1, No. 281, pp.31-50.

European Parliament. (2012), "Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)", pp. 1-99, http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf, (Accessed 29 June 2015).

Greens, J.P.A. (2015), "EU General Data Protection Regulation State of Play and 10 Main Issues", p.1, http://www.janalbrecht.eu/fileadmin/material/Dokumente/Data_protection_state_of_play_10_points_010715.pdf, (Accessed 29 June 2015).

Hoar, S.B. (2001), "Identity Theft: The Crime of the New Millennium", Oregon Law Review, Vol.80, No.4, p.1423.

Information Systems Audit and Control Association (ISACA). (2014), "Risk to Entities Regarding Data Breaches - Lessons from a Brief Case Study", Information Systems Audit and Control Association (ISACA) Journal, Vol.2, p.14.

Kirby, M. (2011), "The History, Achievement and Future of the 1980 OECD Guidelines on Privacy", International Data Privacy Law, Vol.1, No.1, p.6.

Kuner, C. (2011), "Regulation of Transborder Data Flows Under Data Protection and Privacy Law: Past, Present and Future", OECD Digital Economy Papers, No.187, pp.10-11.

Kuneva, M. (2009), "Keynote Speech - Roundtable on Online Data Collection, Targeting and Profiling", p.2, http://europa.eu/rapid/press-release_SPEECH-09-156_en.pdf, (Accessed 27 June 2015).

Kuschewsky, M. (2014), "The New Privacy Guidelines of the OECD: What Changes for Businesses?", Journal of European Competition Law & Practice, Vol.5, No.3, p.147.

Lynch, L. (2013), "EU Data Protection's Paradigm Shift: From Directive to Regulation", p.2, http://www.ey.com/Publication/vwLUAssets/EU_Data_Protections_Paradigm_Shift_From_Drective_to_Regulation/$FILE/EU%20Data%20Protections%20Paradigm%20Shift%20From%20Directive%20to%20Regulation.pdf, (Accessed 29 June 2015).

Michalsons. (2014), "Protection of Personal Information Act - POPI", http://www.michalsons.co.za/protection-of-personal-information-act-popi/11105, (Accessed 27 June 2015).

Moore, A.D. (2008), "Defining Privacy", Journal of Social Philosophy, Vol.39, No.3, p.425.

Organisation for Economic Co-operation and Development (OECD). (1980), "OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data - Annex to the recommendation of the Council of 23 September 1980", pp.1-4.

Organisation for Economic Co-operation and Development (OECD). (2011), "Thirty Years After The OECD Privacy Guidelines", p.10.

Organisation for Economic Co-operation and Development (OECD). (2013), "OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data", pp.1-154.

Republic of South Africa. (2009), "Protection of Personal Information (POPI) Bill", Cape Town and Pretoria: Government Printer, pp.1-50.

Republic of South Africa. (2013), "Protection of Personal Information (POPI) Act (Act 4 of 2013)", Cape Town: Government Printer, No.37067, pp.2-146.

Saunders, K.M. and Zucker, B. (1999), "Counteracting Identity Fraud in the Information Age: The Identity Theft and Assumption Deterrence Act", International Review of Law, Computers & Technology, Vol.13, No.2, p.183.

Stein, P. (2012), "South Africa's EU-style Data Protection Law", Without Prejudice, Vol.12, Issue 10, pp.48-49.

Titus. (2011), "Protecting Personally Identifiable Information (PII) with Classification and Content Inspection", Titus White Paper, p.5.

World Economic Forum (WEF). (2014), "Global Risks 2014", Insight Report, 9th Edition, pp.12-13, http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2014.pdf, (Accessed 27

June 2015).

SAICSIT 2016

Proceedings of the 2016
Annual Research Conference of the
South African Institute of Computer Scientists
and Information Technologists

Editors

Frans F Blauw
Marijke Coetzee
Duncan A Coulter
Elize M Ehlers
Wai Sze Leung
Carl Marnewick
Dustin T van der Haar

26 - 28 September 2016
Johannesburg, South Africa

A Volume in the
ACM International Conference Proceedings Series
ISBN: 978-1-4503-4805-8

Innovate.
Elevate.

ICPS

ACM ISBN: 978-1-4503-4805-8

Association for Computing Machinery

Title:	Proceedings of the 2016 Annual Research Conference of the South African Institute of Computer Scientists and Information Technologists
Short Title:	SAICSIT 2016 – Innovate. Elevate.
Editors:	Frans F Blauw, Marijke Coetzee, Duncan A Coulter, Elize M Ehlers, Wai Sze Leung, Carl Marnewick & Dustin T van der Haar
Location:	Kerzner Unit, School of Tourism and Hospitality (STH), University of Johannesburg, South Africa
Date:	26 - 28 September 2016
ISBN:	978-1-4503-4805-8

Organising Committee

SAICSIT 2016 was organised by the
Academy of Computer Science and Software Engineering at the
University of Johannesburg. South Africa

The conference was organised by a limited committee of people:

General Conference Chair

Marijke Coetzee

Track Chairs

Computer Science

Elize M Ehlers
Duncan A Coulter

Information Systems

Carl Marnewick
Wai Sze Leung

Masters and Doctoral Symposium

Dustin T van der Haar

Review Process

SAICSIT 2016 followed a strict peer review process. Each submission was assessed by at least three reviewers in a double-blind process. No member of the organising committee or reviewers was involved in the review process of papers where they were authors. A total of 116 papers were submitted to SAICSIT 2016 and 45 were accepted for presentation and publication in these proceedings (a 38.8% acceptance rate).

The list of reviewers who participated in this process follows on the next three pages. The SAICSIT 2016 Organising Committee would like to thank each reviewer for their involvement.

List of Reviewers

Name	Affiliation
Bigomokero Antoine Bagula	*University of Western Cape*
Felix Bankole	*University of South Africa*
Tristan Barnett	*University of Johannesburg*
Frans F Blauw	*University of Johannesburg*
Pieter Blignaut	*University of the Free State*
Reinhardt Botha	*Nelson Mandela Metropolitan University*
Adele Botha	*Meraka Institute, CSIR*
Karen Bradshaw	*Rhodes University*
Irwin Brown	*University of Cape Town*
Laurie Butgereit	*Nelson Mandela Metropolitan University*
Michael Cilliers	*University of Johannesburg*
Liezel Cilliers	*University of Fort Hare*
Loek Cleophas	*TU Eindhoven* *Stellenbosch University*
Serena Coetzee	*University of Pretoria*
Jason Cohen	*University of the Witwatersrand*
Alfred Coleman	*University of South Africa*
Deon Cotterrell	*University of Johannesburg*
Michele Cullinan	*University of Johannesburg*
Rossouw de Bruin	*University of Johannesburg*
Carina de Villiers	*University of Pretoria*
Ruth de Villiers	*School of Computing, Unisa*
Lizette de Wet	*University of the Free State*
Nomusa Dlodlo	*Meraka Institute, CSIR*
Lynette Drevin	*North-West University*
Jaco Du Toit	*University of Johannesburg*
Bernardt Duvenhage	*Council for Scientific and Industrial Research*
Mariki Eloff	*University of South Africa*
Jan Eloff	*University of Pretoria*
Stephen Flowerday	*University of Fort Hare*
Steven Furnell	*Plymouth University*
Jaco Geldenhuys	*Stellenbosch University*
Aurona Gerber	*CAIR, Meraka Institute, CSIR*
Leila Goosen	*University of South Africa*

Name	Affiliation
Brian Greaves	*University of Johannesburg*
Scott Hazelhurst	*University of the Witwatersrand*
Marlien Herselman	*Meraka Institute, CSIR* *Nelson Mandela Metropolitan University*
Vincent Horner	*University of South Africa*
Grant Royd Howard	*University of South Africa*
Barry Irwin	*Rhodes University*
Anne Kayem	*University of Cape Town*
Maria Keet	*University of Cape Town*
Ernest Ketcha Ngassam	*University of South Africa*
Caroline Khene	*Rhodes University*
Derrick Kourie	*University of Stellenbosch*
Rodney Stephen Kroon	*Stellenbosch University*
Hennie Kruger	*North-West University*
Anthony Krzesinski	*Stellenbosch University*
Michelle Kuttel	*University of Cape Town*
Stephen Levitt	*University of the Witwatersrand*
Hugo Lotriet	*University of South Africa*
Candice Louw	*University of Johannesburg*
Jude Lubega	*Uganda Technology and Management University*
Philip Machanick	*Rhodes University*
Anthony Maeder	*University of Western Sydney*
Atish Maganlal	*University of Johannesburg*
Katherine Malan	*University of Pretoria*
Patrick Marais	*University of Cape Town*
Linda Marshall	*University of Pretoria*
Muthoni Masinde	*Central University of Technology*
Machdel Matthee	*University of Pretoria*
Sheu Mavee	*University of Johannesburg*
Jan Mentz	*University of South Africa*
Ernest Mnkandla	*University of South Africa*
Deshendran Moodley	*University of KwaZulu-Natal*
Jabu Mtsweni	*University of South Africa*
Kevin Naudé	*Nelson Mandela Metropolitan University*
Kwete Nyandongo	*University of Johannesburg*

Name	Affiliation
Martin Olivier	*University of Pretoria*
Roxanne Piderit	*University of Fort Hare*
Vreda Pieterse	*University of Pretoria*
Nelishia Pillay	*University of KwaZulu-Natal*
Karen Renaud	*University of Glasgow*
Chris Rensleigh	*University of Johannesburg*
Ian Sanders	*University of South Africa*
Shawren Singh	*University of South Africa*
Hanlie Smuts	*MTN*
Fritz Solms	*University of Pretoria*
Ralf C Staudemeyer	*University of Passau*
Ian Strydom	*University Of Pretoria*
Hussein Suleman	*University of Cape Town*
Bobby Tait	*University Of South Africa*
Marita Turpin	*University of Pretoria*
Isabella M. Venter	*University of the Western Cape*
Hein Venter	*University of Pretoria*
Judy van Biljon	*University of South Africa*
Dustin van der Haar	*University of Johannesburg*
Alta van der Merwe	*University of Pretoria*
Etienne van der Poel	*University of South Africa*
Andre van der Poll	*University of South Africa*
Carl van der Westhuizen	*University of Johannesburg*
Jan van Niekerk	*University of Johannesburg*
Johan van Niekerk	*Nelson Mandela Metropolitan University*
Wynand van Staden	*University of South Africa*
Lynette van Zijl	*Stellenbosch University*
Izak van Zyl	*Cape Peninsula University of Technology*
Rossouw von Solms	*Nelson Mandela Metropolitan University*
Bruce Watson	*Stellenbosch University*
George Wells	*Rhodes University*
Janet Wesson	*Nelson Mandela Metropolitan University*

Understanding the Level of Compliance by South African Institutions to the Protection of Personal Information (POPI) Act

Prittish Dala
Department of Computer Science
University of Pretoria
Pretoria, South Africa
+27824909974
xprittishx@gmail.com

Hein S. Venter
Department of Computer Science
University of Pretoria
Pretoria, South Africa
+27834584407
hventer@cs.up.ac.za

ABSTRACT

Privacy entails controlling the use and access to place, location and personal information. In South Africa, the first privacy legislation in the form of the Protection of Personal Information (POPI) Act was signed into law on 26 November 2013. The POPI Act promotes the protection of personal information by South African public and private institutions and specifies the minimum requirements in twelve chapters, which includes eight conditions for lawful processing of personal information. In 2012, CIBECS as part of their *State of Business Data Protection in South Africa* survey assessed, amongst other aspects, how prepared South African institutions were to comply with the then forthcoming protection of personal information legislation. Since that survey, the POPI Bill progressed to an Act and, more recently, in 2015 processes commenced to appoint the Information Regulator (in terms of the legislation), who would be responsible for enforcing the POPI Act. Due to the aforementioned developments and looming enforcement date associated with the POPI Act, this paper assesses the level of understanding of the POPI Act by participants from South African institutions as well as the current level of compliance to the POPI Act. Specifically, the current level of compliance to Condition Seven of the POPI Act, relating to the confidentiality and integrity of electronic personal information, is explored. Furthermore, a view is provided of the financial value associated with electronic personal information maintained as well as the potential impact a data breach of electronic personal information may have on an institution.

CCS Concepts

• Security and privacy;500→Human and societal aspects of security and privacy;300→Privacy protections;500.

Keywords

Protection of personal information; POPI Act; POPI Act research survey; electronic personal information; and compliance.

SAICSIT '16, September 26-28, 2016, Johannesburg, South Africa.
Copyright is held by the owner/author(s). Publication rights licensed to ACM.
ACM 978-1-4503-4805-8/16/09…$15.00
DOI: http://dx.doi.org/10.1145/2987491.2987506

1. INTRODUCTION

The currency of the digital world and the "oil" of the Internet is personal data [1]. Personal data can be bought, sold and traded, creating economic value [2]. Hence, the global risks identified by the World Economic Forum [3] included data loss as a result of data fraud as a major risk within the technology domain. This is due to the advent of the information age which has presented new challenges in terms of preserving personal information [4].

Privacy entails controlling the use and access to place, location and personal information [5]. The value of personal information has increased significantly due to the advent of the information age [4] and this has subsequently resulted in the most prevalent crime of the new millennium, known as "identity theft" [6]. This rampant form of crime, according to the Information Systems Audit and Control Association (ISACA) [7], largely occurs when criminals electronically break into information systems (such as those owned by institutions) to gain access to databases, which allows them to steal personal information such as financial account numbers, addresses or identity numbers.

As a result, legislation in the ambit of the protection of personal information aims to protect individuals against identity theft and offers wide-ranging institutional benefits such as the protection of an institution's brand, image and reputation, enhancing credibility as well as promoting consumer confidence and goodwill [8].

From a South African perspective, legislation in this area took the form of the Protection of Personal Information (POPI) Bill which was first published for comment in 2005 [9]. After undergoing numerous reviews, the POPI Bill [10] was finally enacted and signed into law on 26 November 2013 as the Protection of Personal Information (POPI) Act [11]. Condition Seven of the POPI Act [11] specifies the need for security safeguards to ensure confidentiality and integrity of personal information.

In 2012, CIBECS [12] as part of their *State of Business Data Protection in South Africa* survey assessed, amongst other aspects, how prepared South African institutions were to comply with the then forthcoming legislation addressing the protection of personal information. Since then, the POPI Bill [10] has progressed to an Act [11] and more recently in 2015 processes commenced to appoint the Information Regulator, who would be responsible for enforcing the POPI Act [13]. The appointment of the Information Regulator will lead to an enforcement date for the POPI Act [11], after which South African public and private institutions will have one year to comply with the legislation. Hence, due to the aforementioned developments and the looming enforcement date associated with the POPI Act, this paper through a research survey assesses the current level of compliance to the POPI Act by South African institutions. A specific focus on the level of compliance to Condition Seven of the POPI Act relating to the confidentiality and integrity of electronic personal information will be explored. Furthermore, the contribution of this paper is to provide an overall level of understanding of the POPI Act by participants from South African institutions who completed the research survey. In addition, participants provide a view of the financial value associated with electronic personal information maintained by their respective institutions as well as the potential impact a data breach of electronic personal information may have on their institutions.

This paper is one of a series of papers associated with the author's research relating to the POPI Act, which focuses specifically on the confidentiality and integrity of electronic personal information as required by Condition Seven of the POPI Act, namely:

- A framework of security safeguards for the confidentiality and integrity of electronic personal information as required by Condition Seven of the POPI Act, which has been presented and published.
- The extent to which the European Union and South African privacy legislation addresses the 2013 Organisation for Economic Cooperation and Development (OECD) guidelines on trans-border data flows and the protection of privacy, including eight privacy principles, which has been presented and published.
- Understanding the level of compliance by South African institutions to the POPI Act, which is this current paper.
- The current state of security safeguards within South African institutions, in relation to electronic personal information, to achieve compliance to Condition Seven of the POPI Act, which has been completed and submitted.
- A model of operation to guide the implementation of the security safeguards, as required by Condition Seven of the POPI Act, which is a forthcoming paper.

This paper is structured as follows: Section 2 provides a background of the POPI Act and an overview of the *State of Business Data Protection in South Africa* survey. An overview of the research methodology, research group and research survey results, followed by an analysis of the research survey responses received, is provided in Section 3. Section 4 provides a critical evaluation of the analysis performed in Section 3 by way of key findings, recommendations and comparisons. Section 5 concludes the paper and also presents future work.

2. BACKGROUND

This section provides a background of the POPI Act and an overview of the *State of Business Data Protection in South Africa* survey [12] which assessed, amongst other aspects, how prepared South African institutions were to comply with the then forthcoming protection of personal information legislation.

2.1 South African POPI Act

The POPI Act [11] promotes the protection of personal information by South African public and private institutions and specifies the minimum requirements in 12 chapters, which includes 8 conditions for lawful processing of personal information. Condition Seven of the POPI Act [11] specifically addresses the need to implement security safeguards to ensure the confidentiality and integrity of electronic personal information.

Although the POPI Act was signed into law on 26 November 2013 the enforcement date is still to be announced. However, the "Transitional arrangements" section of the POPI Act [11] contained in Chapter 11 specifies that within 1 year, compliance to the Act should be achieved by public and private institutions in South Africa, unless exemptions, which are gazetted, are granted. In the event of such exemption, however, the time granted to comply may not exceed 3 years.

An external Information Regulator has to be established in terms of Section 39 of the POPI Act [11] to promote, enforce and monitor compliance to the Act. The processes to appoint the Information Regulator commenced in 2015 and are currently underway [13].

According to Michalsons [14], in the event that compliance to the POPI Act is not achieved, members of South African public and private institutions may be fined up to 10 million rand, face imprisonment not exceeding 10 years or receive a combination of a fine and imprisonment. Furthermore, institutions may suffer reputational damage, lose customers and may have to pay out millions in damages due to civil class action [14].

2.2 2012 State of Business Data Protection in South Africa

In 2012, CIBECS [12] as part of their *State of Business Data Protection in South Africa* survey assessed, amongst other aspects, how prepared South African institutions were to comply with the then forthcoming protection of personal information legislation.

The results of the survey revealed that 38% of participants were unsure of the how prepared their institutions were to comply with the then forthcoming protection of personal information legislation. Furthermore, 18% of participants stated that no initiatives were underway to ensure compliance. However, 26% of participants were actively looking at technologies and processes to ensure compliance, while 18% of participants were investigating the requirements but not actively pursuing compliance to the then forthcoming protection of personal information legislation [12].

3. RESEARCH SURVEY AND ANALYSIS

This section provides an overview of the research methodology, research group and research survey results, followed by an analysis of the research survey responses received. The analysis of the responses focused on the following aspects:

- The overall level of understanding of the POPI Act.
- The current level of compliance to the POPI Act.
- The level of compliance to Condition Seven of the POPI Act.
- The financial value associated with electronic personal information as well as the potential impact of a data breach of electronic personal information.

3.1 Research Methodology

The research methodology encompassed a quantitative inferential approach [15], which aims to draw conclusions about a group based on a sample in the form of a research group. This approach was driven by the use of a research survey, which was located at *https://www.surveymonkey.com/r/SAPOPI* and was launched from 1 October 2015 to 15 December 2015. The research survey was completely anonymous and participants were not requested to provide any identifying information such as personal information (title, name, surname and email address) or the name of the institution which they represent. All participants had to electronically provide consent and accept the terms and conditions of the research survey before participating.

3.2 Research Group

The research survey specifically targeted participants at South African institutions who store, process or transmit electronic personal information and who, as a result, are impacted by the POPI Act.

The participants were informed of the research survey via an email that included a link to the research survey as well as social media (Twitter and LinkedIn posts) and the South African Chapter of Information Systems Audit and Control Association (ISACA), who distributed the research survey link to members of the South African chapter. Participants were also able to share the link with other participants within their network. As such, CIBECS assisted by distributing the survey link to participants who were targeted for the 2012 *State of Business Data Protection in South Africa* survey [12].

3.3 Research Survey Results

The research survey was launched on 1 October 2015 and closed on 15 December 2015. During this period, 181 participants completed the survey. However, only 167 research survey responses from participants were considered valid, in that the participant's institution operates in South Africa and maintains electronic personal information and as a result is affected by the POPI Act.

3.4 Research Survey Response Analysis

3.4.1 The Overall Level of Understanding of the Protection of Personal Information (POPI) Act

The overall level of understanding of the POPI Act by the 167 participants from South African institutions is depicted in table 1 below:

Table 1: Overall level of understanding of the POPI Act

How would you rate your overall level of understanding of the Protection of Personal Information (POPI) Act?	Response Count	Response Percentage
None	1	0.6%
Limited	34	20.4%
Basic	74	44.3%
Good	41	24.6%
Excellent	17	10.2%
Total	**167**	**100%**

The majority of participants (44.3%) had a basic overall level of understanding of the POPI Act. This was followed by 24.6% of participants who had a good overall level of understanding as opposed to 10.2% of participants who had an excellent overall level understanding of the POPI Act. A limited overall understanding of the POPI Act was applicable to 20.4% of participants with only 1 participant (0.6%) possessing no overall level understanding of the POPI Act.

3.4.2 The Current Level of Compliance to the Protection of Personal Information (POPI) Act

A critical aspect of this research paper is the assessment of the current level of compliance to the POPI Act by South African institutions as provided by the research survey participants, which is summarised in table 2 below.

Table 2: The current level of compliance to the POPI Act

How would you rate your institution's overall compliance to the POPI Act?	Response Count	Response Percentage
No initiatives under way to ensure compliance	9	5.4%
Formal recognition to comply and a project initiated to ensure compliance (security safeguards identified for implementation)	50	29.9%
Partial compliance in that a project is underway to ensure compliance (partial implementation of security safeguards)	76	45.5%
Full compliance to the POPI Act (full implementation of security safeguards)	18	10.8%
Unsure of my institution's level of overall compliance to the POPI Act	14	8.4%
Total	**167**	**100%**

As per table 2 above, the majority of participants (45.5%) stated that their respective institution was partially complying to the POPI Act, in other words, that a project is underway to ensure compliance and security safeguards are partially implemented. Formal recognition to comply with the POPI Act, and as such a project was initiated to ensure compliance to the legislation, was applicable to 29.9% of the participants. However, 8.4% of participants were unsure of their institutions' level of overall compliance to the POPI Act. Furthermore, 5.4% of participants stated that no initiatives were underway in their institutions to ensure compliance with the POPI Act. However, 10.8% of participants stated that their institutions fully comply with the POPI Act, implying that security safeguards are fully implemented.

3.4.3 The Level of Compliance to Condition Seven of the Protection of Personal Information (POPI) Act

Taking into account the level of overall compliance to the POPI Act the level of compliance to Condition Seven of the POPI Act, specifically relating to the confidentiality and integrity of electronic personal information, was explored as illustrated in table 3 below:

Table 3: The level of compliance to Condition Seven of the POPI Act

How would you rate your institutions overall compliance to ensuring confidentiality (prevention of unauthorised disclosure) and integrity (prevention of unauthorised modification) of electronic personal information as required by the POPI Act?	Response Count	Response Percentage
No initiatives under way to ensure compliance	10	6.0%
Formal recognition to comply and a project initiated to ensure compliance (security safeguards identified for implementation)	48	28.7%
Partial compliance in that a project is underway to ensure compliance (partial implementation of security safeguards)	70	41.9%
Full compliance (full implementation of security safeguards)	27	16.2%
Unsure of my institutions level of overall compliance to ensure confidentiality and integrity of electronic personal information	12	7.2%
Total	**167**	**100%**

The majority of participants (41.9%) stated that their respective institution was partially complying in terms of ensuring confidentiality and integrity of electronic personal information as required by Condition Seven of the POPI Act, in that a project is underway to ensure compliance. There is formal recognition to comply with the ensuring confidentiality and integrity of electronic personal information as required by Condition Seven of the POPI Act and as such a project was initiated to ensure compliance, which was applicable to 28.7% of the participants. However, 7.2% of participants were unsure of their institutions' level of compliance to ensure confidentiality and integrity of electronic personal information as required by Condition Seven of the POPI Act. Furthermore, 6.0% of participants stated that no initiatives were underway in their institutions to ensure confidentiality and integrity of electronic personal information as required by Condition Seven of the POPI Act. However, 16.2% of participants stated that their institutions fully comply with ensuring confidentiality and integrity of electronic personal information as required by Condition Seven of the POPI Act.

3.4.4 The Financial Value Associated with Electronic Personal Information as well as the Potential Impact of a Data Breach of Electronic Personal Information

Participants also provided a view on the financial value associated with the electronic personal information maintained by their respective institutions, as illustrated in table 4 below:

Table 4: The financial value associated with electronic personal information

What do you estimate is the financial value of electronic personal information maintained by your institution?	Response Count	Response Percentage
R0 to R99,999	6	3.6%
R100,000 to R200,000	0	0.0%
R200,001 to R300,000	0	0.0%
R300,001 to R400,000	6	3.6%
R400,001 to R500,000	16	9.6%
R500,001 to R600,000	9	5.4%
R600,001 to R700,000	13	7.8%
R700,001 to R800,000	9	5.4%
R800,001 to R900,000	12	7.2%
R900,001 to R1,000,000	3	1.8%
R1,000,000+	47	28.1%
Do not know the financial value	46	27.5%
Total	**167**	**100%**

In terms of the financial value associated with electronic personal information, the majority of participants (28.1%) assigned a value in excess of 1 million rand. A number of participants (27.5%) did not know the financial value associated with electronic personal information maintained by their respective institutions. However, the remaining 44.4% of participants could allocate a financial value ranging from 0 to 1 million rand. Furthermore, as illustrated in table 5 below, participants provided a view on the potential impact a data breach of electronic personal information may have on their respective institutions.

Table 5: The potential impact of a data breach of electronic personal information

How will a breach/compromise of electronic personal information impact your institution (select the scenario below that will have the highest impact on your institution)?	Response Count	Response Percentage
Loss of jobs	9	5.4%
Reputational damage	129	77.2%
Penalties (financial or imprisonment)	16	9.6%
Failed audits	8	4.8%
No impact	1	0.6%
Not sure	4	2.4%
Total	**167**	**100%**

The highest impact of a data breach of electronic personal information would be reputational damage to the institution, according to 77.2% of participants. This was followed by penalties (financial or imprisonment) which account for 9.6% of participants, loss of jobs which account for 5.4% of participants and failed audits which account for 4.8% of participants. However, 2.4% of participants were unsure of the impact of a data breach of electronic personal information and 1 participant (0.6%) stated that a data breach of electronic personal information would have no impact.

4. CRITICAL EVALUATION OF THE ANALYSIS

This section provides a critical evaluation of the analysis performed in section three of this paper by way of key findings, recommendations and comparisons.

4.1 The Overall Level of Understanding of the Protection of Personal Information (POPI) Act

The overall level of understanding of the POPI Act at the time of the research survey being conducted was at a basic level (44.3% of the participants). As a result, given that the POPI Act is not yet enforceable, there is a window of opportunity that exists to increase the level of understanding from basic to good or excellent in order to successfully drive the initiatives to ensure compliance and address areas of non-compliance.

4.2 The Current Level of Compliance to the Protection of Personal Information (POPI) Act (Comparison Between 2012 and 2015)

In order to compare the level of compliance to the POPI Act by South African institutions in 2015 to the level of compliance shown in 2012 as per the *State of Business Data Protection in South Africa* survey conducted by CIBECS [12] the grouping as illustrated in table 6 below was performed to ascertain the common categories for comparison.

The rationale for ascertaining common categories for comparison is that in 2012 the Protection of Personal Information legislation was still at the stage of a Bill and once it was enacted as the POPI Act, formal initiatives to comply had commenced. In both research surveys, participants stated "No" initiatives were underway to comply or they were "Unsure" of the level of compliance to the protection of personal information legislation, resulting in a direct link in the formulation of the two of the three common categories for comparison. However, the third common category termed "Yes" was formulated by grouping together all activities towards achieving compliance from investigation to formal recognition and partial compliance as well as full compliance to the POPI Act.

Table 6: Formulation of common categories for comparison

CIBECS Category - 2012	Research Survey Category - 2015	Common Category Formulated for Comparison
Investigating the requirements but not actively pursuing compliance - 18%	Formal recognition to comply and a project initiated to ensure compliance (security safeguards identified for implementation) - 29.9%	Yes
Actively looking at technologies and processes to ensure compliance - 26%	Partial compliance in that a project is underway to ensure compliance (partial implementation of security safeguards) - 45.5% Full compliance to the POPI Act (full implementation of security safeguards) - 10.8%	
No initiatives were underway to ensure compliance with the forthcoming protection of personal information legislation - 18%	No initiatives under way to ensure compliance - 5.4%	No
Unsure of the how prepared their institutions were to comply with the forthcoming protection of personal information legislation - 38%	Unsure of my institutions level of overall compliance to the POPI Act - 8.4%	Unsure

The comparison between the current level of compliance to the POPI Act by South African institutions in 2015 to the previous level of compliance as per the 2012 *State of Business Data Protection in South Africa* survey conducted by CIBECS [12] is provided in table 7 below, utilising the common categories formulated in table 6 above:

Table 7: The current level of compliance to the POPI Act (comparison between 2012 and 2015)

Common Category Formulated for Comparison	CIBECS Category - 2012	Research Survey Category - 2015
Yes	44%	86%
No	18%	5.4%
Unsure	38%	8.4%

The research survey conducted in 2015 illustrated a significant increase towards achieving compliance to the POPI Act from 44% to 86% of the participants. This can be attributed to the fact that the POPI Act [11] was signed into law on 26 November 2013 and more recently in 2015 processes commenced to appoint the Information Regulator, who would be responsible for enforcing the POPI Act [13]. The appointment of the Information Regulator will lead to an enforcement date for the POPI Act, after which South African public and private institutions will have one year to comply [11]. It is also encouraging to note the significant decrease in participants who stated "No" initiatives (from 18% to 5.4% of participants) were underway to ascertain the level of compliance or they were "Unsure" of the level of compliance (from 38% to 8.4%) to the POPI Act by their respective institutions.

4.3 Overall Compliance to the Protection of Personal Information (POPI) Act versus Overall Compliance to Ensure Confidentiality and Integrity of Electronic Personal Information as Required By Condition Seven of the POPI Act

An analysis of the overall level of compliance to the POPI Act compared to the overall level of compliance to ensure confidentiality and integrity of electronic personal information as required by Condition Seven of the POPI Act is provided in table 8 below. This analysis is critical to ensure that the compliance initiative does not neglect electronic personal information.

Table 8: Overall compliance to the POPI Act versus overall compliance to ensure confidentiality and integrity of electronic personal information as required by Condition Seven of the POPI Act

Level of Compliance Category	**Overall Compliance to the POPI Act**	**Overall Compliance to Ensuring Confidentiality and Integrity of Electronic Personal Information as Required By Condition Seven of the POPI Act**	**Variance**
No initiatives under way to ensure compliance	5.4%	6.0%	+0.6%
Formal recognition to comply and a project initiated to ensure compliance (security safeguards identified for implementation)	29.9%	28.7%	-1.2%
Partial compliance in that a project is underway to ensure compliance (partial implementation of security safeguards)	45.5%	41.9%	-3.6%
Full compliance to the POPI Act (full implementation of security safeguards)	10.8%	16.2%	5.4%
Unsure of my institutions level of overall compliance to the POPI Act	8.4%	7.2%	-1.2%

In table 8 above, a positive variance reflects the level of compliance in terms of ensuring confidentiality and integrity of electronic personal information for a particular compliance category to be higher than the overall level of compliance to the POPI Act. In comparison, a negative variance reflects the level of compliance in terms of ensuring confidentiality and integrity of electronic personal information for a particular compliance category to be lower than the overall level of compliance to the POPI Act. As such, the positive and negative variance for 4 of the 5 categories do not exceed 5%, as per table 8 above, and this illustrates a degree of alignment between the overall initiative to achieve compliance to the POPI Act and at the same time, to address the requirements of Condition Seven of the POPI Act to ensure confidentiality and integrity of electronic personal information. For example, 8.4% of participants were unsure of the overall level of compliance to the POPI Act and 7.2% of participants were unsure of the level of compliance in ensuring confidentiality and integrity of electronic personal information. One compliance category exceeded 5%, as per table 2 above, and it related to full compliance. This demonstrates that there is a greater level of compliance to ensure confidentiality and integrity of electronic personal information as opposed to the overall level of compliance to the POPI Act. However, this does not pose a major threat as the overall level of compliance to the POPI Act takes into account several other requirements, for example, non-electronic personal information as well as processes for reporting a breach.

4.4 The Financial Value Associated with Electronic Personal Information

The majority of participants (72.5%) associated a financial value to the electronic personal information maintained by their institutions. 28.1% assigned a value in excess of 1 million rand while 44.4% of participants associated a financial value ranging from 0 to 1 million rand. However, the remaining 27.5% of participants could not associate a financial value to the electronic personal information maintained by their respective institutions. This may pose a challenge in terms of justifying the costs associated with the safeguards required to ensure confidentiality and integrity of electronic personal information. For example, if the financial value of electronic personal information is R900 000, the safeguards to ensure confidentiality and integrity of electronic personal information should generally not exceed R900 000. In addition, understanding the financial value of electronic personal information together with the costs of safeguards to ensure confidentiality and integrity of electronic personal information will strengthen the business case relating to the protection of personal information (POPI) compliance initiative. Furthermore, in the event of a data breach of electronic personal information a financial value may be associated with the loss of electronic personal information.

4.5 The Impact of a Data Breach of Electronic Personal Information

Reputational damage to an institution was rated to have the highest impact in the event of a data breach of electronic personal information by 77.2% of participants. This was followed by penalties (financial or imprisonment) which account for 9.6% of participants. Reputational damage will remain a high impact area in the event of a data breach of electronic personal information. However, once the POPI Act is enforced and if not complied with, members of the South African public and private institutions may be fined up to 10 million rand, face imprisonment not exceeding 10 years or receive a combination of a fine and imprisonment [14]. This may lead to an increase in the number of participants who associate the impact of a data breach with penalties (financial or imprisonment).

5. CONCLUSION AND FUTURE WORK

In this paper, the overall level of understanding of the POPI Act by participants from South African institutions was assessed, which revealed that at the time of the research survey being conducted the overall level of understanding of the POPI Act was at a basic level (44.3% of the participants).

In addition, in this paper the current level of compliance to the POPI Act as well as level of compliance to Condition Seven of the Act, specifically relating to the confidentiality and integrity of electronic personal information was explored. The current level of compliance to the POPI Act showed a significant increase from 44% (2012) to 86% (2015). In addition, the overall initiative to ensure compliance with the POPI Act compared to the compliance initiative to address Condition Seven of the Act specifically relating to the confidentiality and integrity of electronic personal information presented a degree of alignment in that neither compliance initiatives were neglected.

Furthermore, in the assessment of financial value associated with electronic personal information the majority of participants (72.5%) were able to associate a financial value to the electronic personal information maintained by their respective institutions. With regard to a potential data breach of electronic personal information, reputational damage to an institution was rated to have the highest impact.

In terms of future work, a model of operation will be proposed to guide the implementation of the security safeguards to ensure confidentiality and integrity of electronic personal information stored, processed and transmitted, as required by Condition Seven of the POPI Act.

6. ACKNOWLEDGMENTS

Thank you to all the participants who completed and further distributed the research survey. Furthermore, thank you to the South African Chapter of Information Systems Audit and Control Association (ISACA), who distributed the research survey link to members of the South African chapter as well as CIBECS who assisted by distributing the survey link to participants who were targeted for the 2012 *State of Business Data Protection in South Africa* survey.

7. REFERENCES

[1] Kuneva, M. (2009), “Keynote Speech - Roundtable on Online Data Collection, Targeting and Profiling”, p.2, http://europa.eu/rapid/press-release_SPEECH-09-156_en.pdf, (Accessed, 6 May 2016).

[2] Ali, A., Eggers, W.D., Hamill, R. and Hersey, J. (2013), “Data as the New Currency - Government’s Role in Facilitating the Exchange”, *Deloitte Review*, Issue 13, p.19.

[3] World Economic Forum (WEF). (2014), “Global Risks 2014”, *Insight Report*, 9th Edition, pp.12-13, http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2014.pdf, (Accessed 7 May 2016).

[4] Saunders, K.M. and Zucker, B. (1999), “Counteracting Identity Fraud in the Information Age: The Identity Theft and Assumption Deterrence Act”, *International Review of Law, Computers & Technology*, Vol.13, No.2, p.183.

[5] Moore, A.D. (2008), “Defining Privacy”, *Journal of Social Philosophy*, Vol.39, No.3, p.425.

[6] Hoar, S.B. (2001), “Identity Theft: The Crime of the New Millennium”, *Oregon Law Review*, Vol.80, No.4, p.1423.

[7] Information Systems Audit and Control Association (ISACA). (2014), “Risk to Entities Regarding Data Breaches - Lessons from a Brief Case Study”, *Information Systems Audit and Control Association (ISACA) Journal*, Vol.2, p.14.

[8] Titus. (2011), “Protecting Personally Identifiable Information (PII) with Classification and Content Inspection”, *Titus White Paper*, p.5.

[9] Stein, P. (2012), “South Africa’s EU-style Data Protection Law”, *Without Prejudice*, Vol.12, Issue 10, pp.48-49.

[10] Republic of South Africa. (2009), “Protection of Personal Information (POPI) Bill”, Cape Town and Pretoria: Government Printer, pp.1-50.

[11] Republic of South Africa. (2013), “Protection of Personal Information (POPI) Act (Act 4 of 2013)”, Cape Town: Government Printer, No.37067, pp.2-146.

[12] CIBECS. (2012), “State of Business Data Protection in South Africa”, http://offers.cibecs.com/state-of-business-data-protection-in-sa, (Accessed, 6 May 2016).

[13] Parliament of the Republic of South Africa. (2015), “Announcements, Tablings and Committee Reports”, Cape Town: Government Printer, No. 70-2015, p.2205.

[14] Michalsons. (2014), “Protection of Personal Information Act - POPI”, http://www.michalsons.co.za/protection-of-personal-information-act-popi/11105, (Accessed, 6 May 2016).

[15] Kothari, C.R. (2004), “Research Methodology: Methods and Techniques”, New Age International, p.5.

PROCEEDINGS OF THE AFRICAN CYBER CITIZENSHIP CONFERENCE 2016 (ACCC2016)

31 October-1 November 2016
Port Elizabeth
South Africa

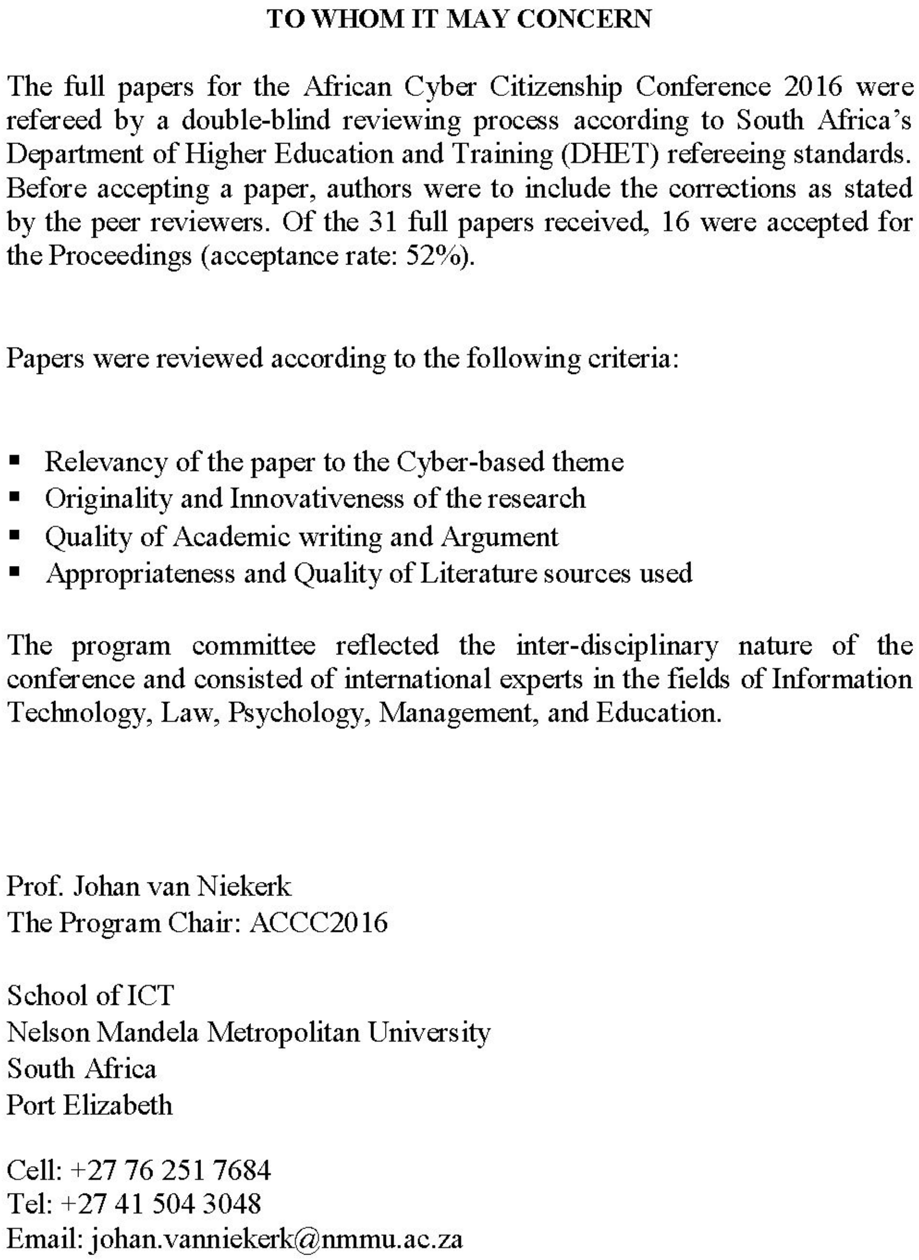
Editor:

J.F. Van Niekerk

Publisher:
Nelson Mandela Metropolitan University
PO Box 77000
Port Elizabeth
6031

Proceedings published at
http://accconference.nmmu.ac.za

ISBN: 978-1-920508-74-6



TO WHOM IT MAY CONCERN

The full papers for the African Cyber Citizenship Conference 2016 were refereed by a double-blind reviewing process according to South Africa's Department of Higher Education and Training (DHET) refereeing standards. Before accepting a paper, authors were to include the corrections as stated by the peer reviewers. Of the 31 full papers received, 16 were accepted for the Proceedings (acceptance rate: 52%).

Papers were reviewed according to the following criteria:

- Relevancy of the paper to the Cyber-based theme
- Originality and Innovativeness of the research
- Quality of Academic writing and Argument
- Appropriateness and Quality of Literature sources used

The program committee reflected the inter-disciplinary nature of the conference and consisted of international experts in the fields of Information Technology, Law, Psychology, Management, and Education.

Prof. Johan van Niekerk
The Program Chair: ACCC2016

School of ICT
Nelson Mandela Metropolitan University
South Africa
Port Elizabeth

Cell: +27 76 251 7684
Tel: +27 41 504 3048
Email: johan.vanniekerk@nmmu.ac.za

Program Committee ACCC 2016

Name	Email	Affiliation
Adrie Stander	adrie.stander@uct.ac.za	University of Cape Town
Anne Karen Seip	annikken@online.no	Finanstilsynet
Aurona Gerber	aurona.gerber@gmail.com	CAIR, University of Pretoria
Carlos Rieder	carlos.rieder@isec.ch	isec ag
Elmarie Kritzinger	kritze@unisa.ac.za	UNISA
Frans Marx	Frans.Marx@nmmu.ac.za	Nelson Mandela Metropolitan University
Gertjan van Stam	g@vanstam.net	SIRDC
Greg Howcroft	greg.howcroft@nmmu.ac.za	Nelson Mandela Metropolitan University
Jacques Ophoff	Jacques.Ophoff@uct.ac.za	University of Cape Town
Jean-Paul Van Belle	Jean-Paul.VanBelle@uct.ac.za	University of Cape Town
Johan van Niekerk	johanvn@nmmu.ac.za	Nelson Mandela Metropolitan University
Karen Renaud	karen.renaud@glasgow.ac.uk	University of Glasgow
Kerry-Lynn Thomson	Kerry-Lynn.Thomson@nmmu.ac.za	Nelson Mandela Metropolitan University
Lech Janczewski	lech@auckland.ac.nz	The University of Auckland
Liezel Cilliers	liezelcilliers@yahoo.com	University of Fort Hare
Lynn Futcher	lynn.futcher@nmmu.ac.za	Nelson Mandela Metropolitan University
Mariana Gerber	mariana@nmmu.ac.za	Nelson Mandela Metropolitan University
Marijke Coetzee	marijkec@uj.ac.za	University of Johannesburg
Marlien Herselman	mherselman@csir.co.za	Meraka Institute, CSIR
Matt Bishop	mabishop@ucdavis.edu	University of California at Davis
Roxanne Piderit	rpiderit@ufh.ac.za	University of Fort Hare
Stephen Flowerday	sflowerday@ufh.ac.za	University of Fort Hare

The Current State of Security Safeguards within South African Institutions to Achieve Compliance to Condition Seven of the POPI Act

P.Dala and H.Venter
Department of Computer Science, University of Pretoria, Pretoria, South Africa
e-mail: xprittishx@gmail.com and hventer@cs.up.ac.za

Abstract

Privacy entails controlling the use and access to place, location and personal information. In South Africa, the first privacy legislation in the form of the Protection of Personal Information (POPI) Act was signed into law on 26 November 2013. The POPI Act promotes the protection of personal information by South African institutions and specifies the minimum requirements in twelve chapters, which includes eight conditions for lawful processing of personal information. Condition Seven of the POPI Act makes specific provision for security safeguards to ensure confidentiality and integrity of personal information. In a previous research paper, the authors proposed a framework that included a selection of security safeguards across 3 domains (management, technical and operational) from several leading practices to facilitate the achievement and maintenance of compliance with Condition Seven of the POPI Act, with a specific focus on confidentiality and integrity of electronic personal information stored, processed or transmitted. However, the applicability, extent of implementation and completeness of the security safeguards across the 3 domains has not been explored. Hence, this paper, through an assessment of the current state of security safeguards done via participants from South African institutions, provides an evaluation of applicability, extent of implementation and completeness of the security safeguards across the 3 domains, previously proposed by the authors, to ensure confidentiality and integrity of electronic personal information as required by Condition Seven of the POPI Act.

Keywords

Protection of personal information, POPI Act, POPI Act research survey, electronic personal information, security safeguards.

1. Introduction

The currency of the digital world and the "oil" of the Internet is personal data (Kuneva, 2009). Personal data can be bought, sold and traded creating economic value (Ali *et al.* 2013). Hence, the global risks identified by the World Economic Forum (2014) included data loss as a result of data fraud as a major risk within the technology domain. This is due to the advent of the information age which has presented new challenges in terms of preserving personal information (Saunders and Zucker, 1999).

Privacy entails controlling the use and access to place, location and personal information (Moore, 2008). The value of personal information has increased significantly due to the advent of the information age (Saunders and Zucker, 1999) and this has subsequently resulted in the most prevalent crime of the new millennium known as "identity theft" (Hoar, 2001). This rampant form of crime according to the Information Systems Audit and Control Association (ISACA) (2014) largely occurs when criminals electronically "break into" information systems (such as those owned by institutions) to gain access to databases, which allows them to steal personal information such as financial account numbers, addresses or identity numbers.

As a result, legislation in the ambit of the protection of personal information aims to protect individuals against identity theft and offers wide-ranging institutional benefits such as the protection of an institution's brand, image and reputation, enhancing the credibility of an institution as well as promoting consumer confidence and goodwill (Titus, 2011).

From a South African perspective, legislation in this area took the form of the Protection of Personal Information (POPI) Bill which was first published for comment in 2005 (Stein, 2012). After undergoing numerous reviews, the POPI Bill (2009) was finally enacted and signed into law on 26 November 2013 as the Protection of Personal Information (POPI) Act (2013). Condition Seven of the POPI Act (2013) specifies the need for security safeguards to ensure confidentiality and integrity of personal information.

In a previous research paper (2015), the authors proposed a framework that included a selection of security safeguards across 3 domains (management, operational and technical) from several leading practices to ensure confidentiality and integrity of electronic personal information as required by Condition Seven of the POPI Act. However, the applicability, extent of implementation and completeness of the security safeguards across the 3 domains (management, operational and technical) has not been explored. Applicability explores if the security safeguard is used within an institution. The extent of implementation assesses if the security safeguard is fully implemented, partially implemented or is being considered for implementation. Lastly, completeness assesses if there are any additional security safeguards, which the authors may not have considered to ensure confidentiality and integrity of electronic personal information as required by Condition Seven of the POPI Act. Hence, the contribution of this paper, through an assessment of the current state of security safeguards done via participants from South African institutions, is to provide an evaluation of applicability, extent of implementation and completeness of the security safeguards across the 3 domains (management, operational and technical), previously proposed by the authors, to ensure confidentiality and integrity of electronic personal information as required by Condition Seven of the POPI Act.

This paper is one of a series of papers associated with the authors' research relating to the POPI Act, which focuses specifically on the confidentiality and integrity of electronic personal information as required by Condition Seven of the POPI Act, namely:

A framework of security safeguards for the confidentiality and integrity of electronic personal information as required by Condition Seven of the POPI Act, which has been presented and published.

The extent to which the European Union and South African privacy legislation addresses the 2013 OECD guidelines on trans-border data flows and the protection of privacy, including eight privacy principles, which has been presented and published.

Understanding the level of compliance by South African institutions to the POPI Act, which has been completed and submitted.

The current state of security safeguards within South African institutions, in relation to electronic personal information, to achieve compliance to Condition Seven of the POPI Act, which is this paper.

A model of operation to guide the implementation of the security safeguards, as required by Condition Seven of the POPI Act, which is a forthcoming paper.

The paper is structured as follows: Section 2 provides a background of the POPI Act as well as the selection of security safeguards across the 3 domains (management, operational and technical), previously proposed by the authors, to ensure confidentiality and integrity of electronic personal information, as required by Condition Seven of the POPI Act. An overview of the research methodology, research group and research survey results followed by an analysis of the research survey responses received is provided in Section 3. Section 4 provides key findings and recommendations. Section 5 concludes the paper and also presents future work.

2. Background

This section provides a background of the POPI Act as well as the selection of security safeguards across the 3 domains (management, operational and technical), previously proposed by the authors, to ensure confidentiality and integrity of electronic personal information as required by Condition Seven of the POPI Act.

2.1. South African Protection of Personal Information Act

The POPI Act (2013) promotes the protection of personal information by South African institutions and specifies the minimum requirements in 12 chapters, which includes 8 conditions for lawful processing of personal information. Although the POPI Act was signed into law on 26 November 2013 the enforcement date of the Act is still to be announced.

2.2. Selection of Security Safeguards

Condition Seven of the POPI Act (2013) specifies the need for security safeguards to ensure confidentiality and integrity of personal information.

In a previous research paper, the authors (2015) proposed a framework that included a selection of security safeguards across management, operational and technical domains, to facilitate the achievement and maintenance of compliance with Condition Seven of the POPI Act, with a specific focus on preventing unauthorised disclosure (maintaining confidentiality) and modification (ensuring integrity) of electronic personal information stored, processed or transmitted. The management domain accounted for 5 security safeguards, namely information security governance, risk management, information security policy, supplier and service level management and business continuity management. This was followed by the operational domain which accounted for 6 security safeguards, namely security procedures and processes, baseline infrastructure security standards, security awareness and training, security monitoring, incident and reporting, security assessment and disaster recovery. The remaining 9 security safeguards formed part of the technical domain, namely network segmentation, encrypted data channels, server and network component security, workstation and laptop security, file integrity, firewalls, physical and environmental security, centralised audit logging, data loss prevention.

3. Research survey and analysis

This section provides an overview of the research methodology, research group, and research survey results followed by an analysis of the research survey responses received via participants from South African institutions in terms of the applicability, extent of implementation and completeness of the security safeguards across the management, operational and technical domains.

.

3.1. Research methodology

The research methodology encompassed a quantitative inferential approach (Kothari, 2004), which aims to draw conclusions about a group based on a sample in the form of a research group. This approach was driven by the use of a research survey, which was located at *https://www.surveymonkey.com/r/SAPOPI* and was launched from 1 October 2015 to 15 December 2015. The research survey was anonymous and participants were not requested to provide any identifying information such as personal information (title, name, surname and email address) or to disclose the name of their institution. Participants electronically provided consent before participating in the research survey.

3.2. Research group

The research survey specifically targeted participants at South African institutions who store, process or transmit electronic personal information and who, as a result, are impacted by the POPI Act.

The participants were informed of the research survey via an email that included a link to the research survey as well as social media (Twitter and LinkedIn posts) and the South African Chapter of Information Systems Audit and Control Association (ISACA), who distributed the research survey link to members of the South African chapter. Participants were also able to share the link within their network. As such, CIBECS assisted by distributing the research survey link to participants who were targeted for the 2012 *State of Business Data Protection in South Africa* survey that assessed, amongst other aspects, how prepared South African institutions were to comply with the forthcoming protection of personal information legislation, which at that stage took the form of the POPI Bill.

3.3. Research survey results

181 participants completed the research survey. However, only 167 research survey responses from participants were considered valid (participants were required to represent a South African institution that maintains electronic personal information and as a result is affected by the POPI Act).

3.4. Research survey response analysis - Applicability of security safeguards

In terms of assessing the applicability of security safeguards, participants were asked if the security safeguards across the 3 domains were applicable (that is, used within their institutions) or not applicable to their institutions, as it relates to to ensuring confidentiality and integrity of electronic personal information as required by Condition Seven of the POPI Act, as illustrated in table 1 below:

Security safeguard domain	Security safeguard applicable to my institution (response count)	Security safeguard applicable to my institution (response percentage)	Security safeguard not applicable to my institution (response count)	Security safeguard not applicable to my institution (response percentage)
Average - Management	165.00	98.80%	2.00	1.20%
Average - Operational	163.17	97.70%	3.83	2.30%
Average - Technical	164.56	98.54%	2.44	1.46%
Overall Average - All Domains	**164.25**	**98.35%**	**2.75**	**1.65%**

Table 1: Applicability of security safeguards

As per table 1 above, an average of 98.35% of participants stated that the security safeguards across the management, operational and technical domains were applicable to their respective institutions in that these are either being considered for implementation or already partially or fully implemented. However, an average of 1.65% participants stated that security safeguards across the management, operational and technical domains were not applicable to their respective institutions.

3.5. Research survey response analysis - Extent of implementation of security safeguards

The extent of implementation of the security safeguards across the 3 domains in terms of full implementation, partial implementation or being considered for implementation, applicable to the average of 98.35% of participants is illustrated in table 2 below:

Security safeguard domain	Security safeguard considered (response count)	Security safeguard considered (response percentage)	Security safeguard partially implemented (response count)	Security safeguard partially implemented (response percentage)	Security safeguard fully implemented (response count)	Security safeguard in place and fully implemented (response percentage)
Average - Management	28.40	17.01%	79.00	47.31%	57.60	34.49%

Security safeguard domain	Security safeguard considered (response count)	Security safeguard considered (response percentage)	Security safeguard partially implemented (response count)	Security safeguard partially implemented (response percentage)	Security safeguard fully implemented (response count)	Security safeguard in place and fully implemented (response percentage)
Average - Operational	34.17	20.46%	87.83	52.59%	41.17	24.65%
Average - Technical	46.56	27.88%	81.67	48.90%	36.33	21.76%
Overall Average - All Domains	**38.30**	**22.93%**	**82.85**	**49.61%**	**43.10**	**25.81%**

Table 2: Extent of implementation of security safeguards

An average of 49.61% of participants, as per table 2 above, revealed partial implementation of the security safeguards across the 3 domains within their institutions. In addition, an average of 25.81% of participants stated that the security safeguards across the 3 domains were fully implemented in their institutions. However, an average of 22.93% of participants stated that the security safeguards across the 3 domains are still being considered within their institutions for implementation.

3.6. Research survey response analysis - Completeness of security safeguards

To assess completeness, the 167 participants were asked to assess if there are any additional security safeguards to the selection of security safeguards, which the authors may have not considered to ensure confidentiality and integrity of electronic personal information as required by Condition Seven of the POPI Act. 150 participants (89.8%) did not provide additional safeguards that are being considered or implemented (partially or fully) by their institutions. However, 17 participants (10.2%) indicated that there were security safeguards that their institutions are considering or implementing (partially or fully) in addition to the selection of security safeguards proposed by the authors. From these 17 responses, 6 were invalid in that they did not provide accurate and sufficient information for further consideration. However, the remaining 11 of the 17 responses, as listed in table 3 below, provided accurate and sufficient information for further consideration:

No.	Safeguards suggested by participants	No.	Safeguards suggested by participants
1	Database level encryption	7	Next generation firewall
2	Encryption	8	File integrity hashing value validation
3	Payment card industry data security standard (PCI DSS)	9	Firmware embedded basic input output system (BIOS) based persistent and remote asset tracking Data and device security
4	International standards and frameworks	10	We acquired an enterprise wide IT system to protect the electronic information
5	Security standards	11	Wi-Fi networks
6	Mobile device management		

Table 3: Security safeguards suggested by participants

An impact analysis of the 11 valid responses (table 3 above) as depicted in table 4 below was conducted to assess the completeness of the security safeguards proposed by the authors, to ensure confidentiality and integrity of electronic personal information. The impact analysis entailed grouping similar responses from the 11 valid responses and then assessing the responses in terms of either impacting or not impacting the security safeguards proposed by the authors. A response was considered to impact the security safeguards proposed by the authors, if it introduced new security safeguards or resulted in changes to the name of a security safeguard or an update of the description associated with a security safeguard. In comparison, a response was considered not to have an impact on the security safeguards proposed by the authors, if it resulted in no change at all as the current selection of security safeguards adequately address the information provided by a response. The result of the impact analysis for each grouping of responses was supported by a rationale. Furthermore, all responses considered to impact the security safeguards proposed by the authors, was supported by a relevant action aimed at capturing the change required to the affected security safeguards.

Security Safeguards Suggested by Participants	Impact (Yes/No), Rationale and Action Required (Yes/No)
Response 1: Database level encryption ***Response 2:*** Encryption ***Response 9:*** Data security	***Impact (Yes/No):*** Yes - Current security safeguards (Encrypted data channels)
	Rationale: Encryption is only addressed from a data channel perspective by the encrypted data channels security safeguard.
	Action Required (Yes/No): Yes - Rename the “Encrypted data channels”security safeguard to “Encryption” and update the description to address encryption holistically from a data security perspective to cover data transmission (data channels) and storage (databases).
Response 3: Payment card	***Impact (Yes/No):*** No
	Rationale: Credit card information is considered personal information however

Security Safeguards Suggested by Participants	Impact (Yes/No), Rationale and Action Required (Yes/No)
industry data security standard (PCI-DSS)	PCI-DSS is a standard specifically for credit card information (PCI Security Standards Council, 2016) and does not apply to institutions who have personal information such as names, surnames and email addresses of clients but no credit card information. As a result, PCI-DSS will not result in an additional security safeguard or an amendment to the security safeguards proposed. However, compliance to the PCI-DSS standard will encompass the implementation of the majority of the security safeguards proposed.
	Action Required (Yes/No): No
Response 4: International standards and frameworks ***Response 5:*** Security standards	***Impact (Yes/No):*** No
	Rationale: The baseline infrastructure security standards safeguard addresses security standards. Furthermore, the security safeguards includes the need for an information security policy, security procedures and processes as well as baseline infrastructure security standards, which should ideally be based on international standards and frameworks to prevent re-inventing the wheel. For example, the information security policy may be based on International Standards Organisation (ISO) 27001.
	Action Required (Yes/No): No
Response 6: Mobile device management ***Response 9:*** Device security	***Impact (Yes/No):*** Yes - Current security safeguards (workstation and laptop security as well as data loss prevention).
	Rationale: Workstation and laptop security makes no provision for mobile devices. Furthermore, data end points for data loss prevention are limited to workstations and laptops.
	Action Required (Yes/No): Yes - Rename the security safeguard "Workstation and laptop security" to "Workstation, laptop and mobile device security" and update the description of the security safeguard to include security of mobile devices. In addition, update the description of the "Data loss prevention" security safeguard to include mobile devices as data end points.
Response 7: Next generation firewall	***Impact (Yes/No):*** Yes - Current security safeguards (file integrity).
	Rationale: Firewalls independent of vendor or technology is addressed by the current security safeguards (firewall).
	Action Required (Yes/No): No
Response 8: File integrity hashing value validation	***Impact (Yes/No):*** No
	Rationale: File integrity is addressed by the file integrity security safeguard, with no provision for hash value validation.
	Action Required (Yes/No): Yes - Update the description of the "File integrity" security safeguard to include hash value validation.
Response 9: Firmware embedded basic input output system (BIOS) based persistent and remote asset tracking	***Impact (Yes/No):*** Yes - Current security safeguards (Security monitoring, incident and reporting, workstation and laptop security as well as data loss prevention).
	Rationale: Yes - Security monitoring, incident and reporting safeguard as well as the workstation and laptop security and data loss prevention safeguards did not take into account asset tracking.
	Action Required (Yes/No): Yes - Update the description of the security monitoring, incident and reporting safeguard to include persistent and remote asset tracking. In addition, the workstation and laptop security safeguard description to be updated to include firmware BIOS based tracking on supported workstations, laptops and mobile devices. Furthermore, the data loss prevention safeguard to enable tracking of assets via data end points, if firmware BIOS based asset tracking is not supported on workstations, laptops or mobile devices.
Response 10: We acquired an enterprise wide IT system to	***Impact (Yes/No):*** No
	Rationale: Enterprise wide IT system is open to interpretation and could be a data loss prevention (DLP) system or a security incident event and monitoring (SIEM) system. Both the DLP and SIEM systems are addressed by the current security

Security Safeguards Suggested by Participants	Impact (Yes/No), Rationale and Action Required (Yes/No)
protect the electronic information	safeguards (Data loss prevention and security monitoring, incident and reporting).
	Action Required (Yes/No): No
Response 11: Wi-Fi networks	***Impact (Yes/No):*** Yes - Current security safeguards (network segmentation as well as server and network component security).
	Rationale: The network segmentation as well as the server and network component security safeguards do not make a distinction between wired and wireless networks.
	Action Required (Yes/No): Yes - Update the description of the "Network segmentation" and "Server and network component security" safeguards to state that the security safeguards are applicable to any form of network may it be wired and wireless or a combination thereof.

Table 4: Impact analysis of the security safeguards suggested by participants

As a result of the aforementioned impact analysis in table 4 above, based on the 11 valid responses, 5 responses had no impact on the security safeguards previously proposed by authors as supported by the rationale provided. However, 6 of the 11 valid responses had an impact on the selection of security safeguards previously proposed by authors, in that it did result in updates to the security safeguards but no additional security safeguards were identified.

4. Critical evaluation of the analysis

This section provides a critical evaluation of the analysis performed in section 3 of this paper by way of key findings and recommendations.

4.1. Applicability of security safeguards

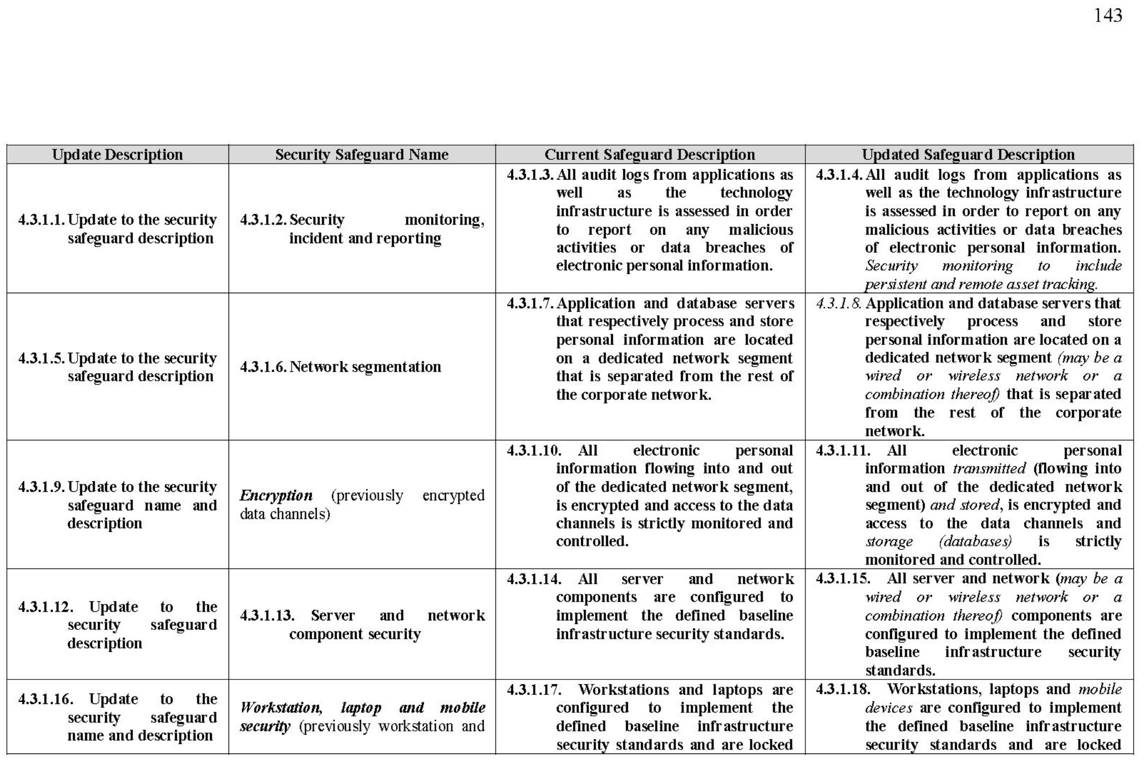
An average of 98.35% of participants stated that security safeguards across the management, operational and technical domains, proposed by the authors, were applicable to their respective institutions (either being considered for implementation or already partially or fully implemented). An average of 1.65% of participants stated that security safeguards across the management, operational and technical domains were not applicable to their respective institutions. Certain security safeguards may not be applicable in the event where the institution has compensating safeguards (other alternative security safeguards to ensure confidentiality and integrity of electronic personal information) in place. However, in the event that the confidentiality and integrity of electronic personal information may be compromised due to the lack of a security safeguard, it is recommended that the security safeguards identified as not applicable to the institution across the management, operational and technical domains be re-considered for implementation to mitigate the risk of disclosure and modification of electronic personal information as well as to ultimately ensure compliance to Condition Seven of the POPI Act.

4.2. Extent of implementation of security safeguards

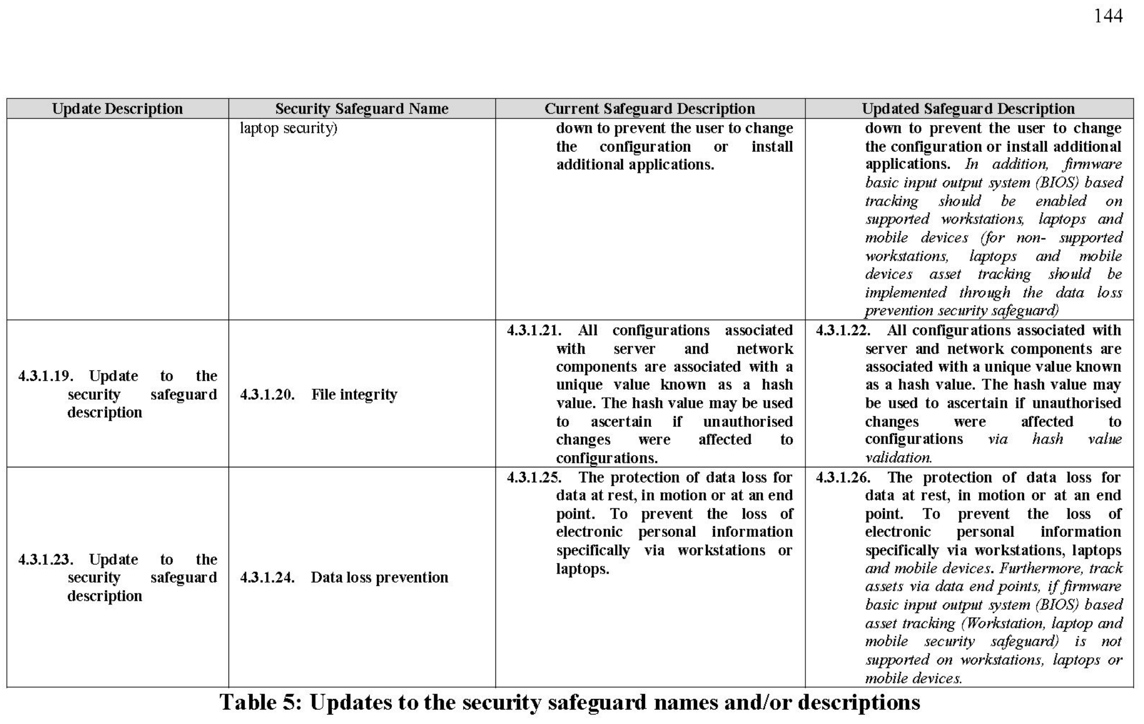
At the time of the research survey being conducted an average of 25.81% of the 98.35% of participants stated that security safeguards across the management, operational and technical domains were fully implemented in their institution. However, security safeguards across the management, operational and technical domains were partially implemented (average of 49.61% of the 98.35% participants) or being considered for implementation (average of 22.93% of the 98.35% of participants). Given that the POPI Act is not yet enforceable, the progress made by South African institutions is considered acceptable in that the implementation of certain of the security safeguards account for a combined average of 75.42% of the 98.35% of participants (partial implementation - 49.61% and full implementation - 25.81%). South African institutions should aim to achieve full implementation of the security safeguards in order to contribute towards the achievement of ensuring compliance to Condition Seven of the POPI Act as well as the overall POPI Act. As a result, the security safeguards that have been fully implemented can be continuously monitored to ensure that the confidentiality and integrity of electronic personal information is preserved, while the security safeguards that have been partially implemented should be fully implemented. Similarly, the security safeguards that are being considered for implementation should be prioritised and implemented in the most effective and efficient manner in order to achieve compliance to Condition Seven of the POPI Act as well as the overall POPI Act.

4.3. Completeness of security safeguards

From a completeness perspective, no additional security safeguards were added to the selection of security safeguards previously proposed by the authors to ensure confidentiality and integrity of electronic personal information. However, based on the information provided by participants in terms of the responses received, driven by themes such as encryption, mobile devices and asset tracking, the names of 2 security safeguards (workstation and laptop security changed to workstation, laptop and mobile security as well as encrypted data channels changed to encryption) were updated. In addition, the description associated with 7 security safeguards were updated. The aforementioned updates are illustrated in italics within table 5 below:



Update Description	Security Safeguard Name	Current Safeguard Description	Updated Safeguard Description
4.3.1.1. Update to the security safeguard description	**4.3.1.2. Security monitoring, incident and reporting**	**4.3.1.3. All audit logs from applications as well as the technology infrastructure is assessed in order to report on any malicious activities or data breaches of electronic personal information.**	**4.3.1.4. All audit logs from applications as well as the technology infrastructure is assessed in order to report on any malicious activities or data breaches of electronic personal information.** *Security monitoring to include persistent and remote asset tracking.*
4.3.1.5. Update to the security safeguard description	**4.3.1.6. Network segmentation**	**4.3.1.7. Application and database servers that respectively process and store personal information are located on a dedicated network segment that is separated from the rest of the corporate network.**	*4.3.1.8.* **Application and database servers that respectively process and store personal information are located on a dedicated network segment** *(may be a wired or wireless network or a combination thereof)* **that is separated from the rest of the corporate network.**
4.3.1.9. Update to the security safeguard name and description	***Encryption*** (previously encrypted data channels)	**4.3.1.10. All electronic personal information flowing into and out of the dedicated network segment, is encrypted and access to the data channels is strictly monitored and controlled.**	**4.3.1.11. All electronic personal information** *transmitted* **(flowing into and out of the dedicated network segment)** *and stored*, **is encrypted and access to the data channels and** *storage (databases)* **is strictly monitored and controlled.**
4.3.1.12. Update to the security safeguard description	**4.3.1.13. Server and network component security**	**4.3.1.14. All server and network components are configured to implement the defined baseline infrastructure security standards.**	**4.3.1.15. All server and network (***may be a wired or wireless network or a combination thereof)* **components are configured to implement the defined baseline infrastructure security standards.**
4.3.1.16. Update to the security safeguard name and description	***Workstation, laptop and mobile security*** (previously workstation and	**4.3.1.17. Workstations and laptops are configured to implement the defined baseline infrastructure security standards and are locked**	**4.3.1.18. Workstations, laptops and** *mobile devices* **are configured to implement the defined baseline infrastructure security standards and are locked**



Update Description	Security Safeguard Name	Current Safeguard Description	Updated Safeguard Description
	laptop security)	**down to prevent the user to change the configuration or install additional applications.**	**down to prevent the user to change the configuration or install additional applications.** *In addition, firmware basic input output system (BIOS) based tracking should be enabled on supported workstations, laptops and mobile devices (for non- supported workstations, laptops and mobile devices asset tracking should be implemented through the data loss prevention security safeguard)*
4.3.1.19. Update to the security safeguard description	**4.3.1.20. File integrity**	**4.3.1.21. All configurations associated with server and network components are associated with a unique value known as a hash value. The hash value may be used to ascertain if unauthorised changes were affected to configurations.**	**4.3.1.22. All configurations associated with server and network components are associated with a unique value known as a hash value. The hash value may be used to ascertain if unauthorised changes were affected to configurations** *via hash value validation.*
4.3.1.23. Update to the security safeguard description	**4.3.1.24. Data loss prevention**	**4.3.1.25. The protection of data loss for data at rest, in motion or at an end point. To prevent the loss of electronic personal information specifically via workstations or laptops.**	**4.3.1.26. The protection of data loss for data at rest, in motion or at an end point. To prevent the loss of electronic personal information specifically via workstations, laptops** *and mobile devices. Furthermore, track assets via data end points, if firmware basic input output system (BIOS) based asset tracking (Workstation, laptop and mobile security safeguard) is not supported on workstations, laptops or mobile devices.*

Table 5: Updates to the security safeguard names and/or descriptions

The updates to the security safeguard names and descriptions as reflected in table 5 above will be taken in account when the model of operation to guide the implementation of security safeguards to ensure confidentiality and integrity of electronic personal is to be defined by the authors.

5. Conclusion and future work

In this paper, the applicability, extent of implementation and completeness of the security safeguards across the management, operational and technical domains, proposed by the authors, through an assessment of participants from South African institutions was explored.

From an applicability and extent of implementation perspective, the security safeguards across the management, operational and technical domains, proposed by the authors, were widely used by South African institutions in that an average of 98.35% of participants stated that security safeguards across the 3 domains were applicable to their respective institutions and the security safeguards are either being considered for implementation (average of 22.93% of the 98.35% of participants) or already partially (average of 49.61% of the 98.35% of participants) or fully implemented (average of 25.81% of the 98.35% of participants).

In terms of the completeness of the security safeguards proposed by the authors, no additional security safeguards were added to ensure confidentiality and integrity of electronic personal information. However, the names and descriptions of specific security safeguards were updated based on the information provided by participants. These updates are to be factored, as part of future work, into the model of operation which aims to guide the implementation of the security safeguards to ensure confidentiality and integrity of electronic personal information stored, processed and transmitted, as required by Condition Seven of the POPI Act (2013).

6. Acknowledgements

Thank you to all of the participants who completed and further distributed the research survey. Furthermore, thank you to the South African Chapter of Information Systems Audit and Control Association (ISACA), who distributed the research survey link to members of the South African chapter as well as CIBECS who assisted by distributing the survey link to participants who were targeted for the 2012 *State of Business Data Protection in South Africa* survey.

7. References

Ali, A., Eggers, W.D., Hamill, R. and Hersey, J. (2013), “Data as the New Currency - Government’s Role in Facilitating the Exchange”, *Deloitte Review*, Issue 13, p.19.

CIBECS. (2012), “State of Business Data Protection in South Africa”, http://offers.cibecs.com/state-of-business-data-protection-in-sa, (Accessed, 6 May 2016).

Dala, P. and Venter, H. (2015), “A Framework of Security Safeguards for Confidentiality and Integrity of Electronic Personal Information”, *Proceedings of the 10th International Conference on Cyber Warfare and Security (ICCWS) 2015*, Kruger National Park, South Africa, pp.415-424.

Hoar, S.B. (2001), “Identity Theft: The Crime of the New Millennium”, *Oregon Law Review*, Vol.80, No.4, p.1423.

Information Systems Audit and Control Association (ISACA). (2014), “Risk to Entities Regarding Data Breaches - Lessons from a Brief Case Study”, *Information Systems Audit and Control Association (ISACA) Journal*, Vol.2, p.14.

Kothari, C.R. (2004), “Research Methodology: Methods and Techniques”, New Age International, p.5.

Kuneva, M. (2009), “Keynote Speech - Roundtable on Online Data Collection, Targeting and Profiling”, p.2, http://europa.eu/rapid/press-release_SPEECH-09-156_en.pdf, (Accessed 27 June 2015).

Moore, A.D. (2008), “Defining Privacy”, *Journal of Social Philosophy*, Vol.39, No.3, p.425.
PCI Security Standards Council (PCI-SSC). (2016), “PCI Security”, https://www.pcisecuritystandards.org/pci_security/, (Accessed 3 June 2016).

Republic of South Africa. (2009), “Protection of Personal Information (POPI) Bill”, Cape Town and Pretoria: Government Printer, pp.1-50.

Republic of South Africa. (2013), “Protection of Personal Information (POPI) Act (Act 4 of 2013)”, Cape Town: Government Printer, No.37067, pp.2-146.

Saunders, K.M. and Zucker, B. (1999), “Counteracting Identity Fraud in the Information Age: The Identity Theft and Assumption Deterrence Act”, *International Review of Law, Computers & Technology*, Vol.13, No.2, p.183.

Stein, P. (2012), “South Africa’s EU-style Data Protection Law”, *Without Prejudice*, Vol.12, Issue 10, pp.48-49.

Titus. (2011), “Protecting Personally Identifiable Information (PII) with Classification and Content Inspection”, *Titus White Paper*, p.5.

World Economic Forum (WEF). (2014), “Global Risks 2014”, Insight Report, 9th Edition,

pp.12-13, http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2014.pdf, (Accessed 3 June 2016).

BIBLIOGRAHY

Alfreds, D. (2016). “SA Fails to Make Data Breaches Public - Expert". *Fin24*. [Online]. Available: http://www.fin24.com/Tech/Cyber-Security/sa-fails-to-make-data-breaches-public-expert-20160226.

Ali, A., Eggers, W.D., Hamill, R. and Hersey, J. (2013). “Data as the New Currency - Government’s Role in Facilitating the Exchange”, *Deloitte Review*, Issue 13, p.19.

Anandarajan, M., D’Ovidio, R. and Jenkins, A. (2013). "Safeguarding Consumers Against Identity-Related Fraud: Examining Data Breach Notification Legislation Through the Lens of Routine Activity Theory", *International Data Privacy Law*, Vol.3, No.1, p.59.

Anusree, M.R., Mohapatra, S. and Sreejesh, S. (2014). “Business Research Design: Exploratory, Descriptive and Causal Designs”, *Business Research Methods*, Springer International Publishing, pp.25-103.

Banisar, D. and Davies, S. (Unknown). “Privacy and Human Rights - An International Survey of Privacy Laws and Practice”, *Global Internet Liberty Campaign*. [Online]. Available: http://gilc.org/privacy/survey/intro.html.

Birnhack, M.D. (2008). “The EU Data Protection Directive: An Engine of a Global Regime”, *Computer Law & Security Review*, Vol.24, Issue 6, pp.508-520.

Botha, J., Eloff, M.M. and Swart, I. (2015). “Evaluation of Online Resources on the Implementation of the Protection of Personal Information Act in South Africa”, *Proceedings of the 10th International Conference on Cyber Warfare and Security*, Kruger National Park, South Africa, 24-25 March 2015, p.41.

British Standards Institute (BSI). (2005). “BS ISO/IEC 27001:2005: Information Technology - Security Techniques - Information Security Management Systems - Requirements”, *First Edition*, p.VI and pp.1-33.

British Standards Institute (BSI). (2013). “ISO 9001 It's in the Detail - Your Implementation Guide”, p.5. [Online]. Available: https://www.bsigroup.com/Documents/iso-9001/resources/BSI-ISO-9001-implementation-guide.pdf.

British Standards Institute (BSI). (2014). “The Business Improvement Handbook”, *Fourth Edition*, p.6.

Chivers, D. and Kafouris, D. (2013). “Getting with the POPI Programme”, *Deloitte*. [Online]. Available: http://www.itweb.co.za/index.php?option=com_content&view=article&id=69449.

CIBECS. (2012). “State of Business Data Protection in South Africa”, pp.3-6. [Online]. Available: http://offers.cibecs.com/state-of-business-data-protection-in-sa.

Clarke, R. (1997 and 2013). “Introduction to Dataveillance and Information Privacy, and Definitions of Terms”. [Online]. Available: http://www.rogerclarke.com/DV/Intro.html.

Clarke, R. (2006). “What’s Privacy”. [Online]. Available: http://www.rogerclarke.com/DV/Privacy.html.

De Bruyn, M. (2014). “The Protection of Personal Information (POPI) Act - Impact on South Africa”, *International Business and Economics Research Journal*, Vol.13, No.6, p.1315.

DLA Piper. (2016). “Data Protection Laws of the World”, pp.3-519. [Online]. Available: https://www.dlapiperdataprotection.com/system/modules/za.co.heliosdesign.dla.lotw.data_protection/functions/handbook.pdf?country=all.

DLA Piper. (2017). “Compare Data Protection Laws around the World”. [Online]. Available: https://www.dlapiperdataprotection.com/index.html.

Dowling Jr, D.C. (2009). “International Data Protection and Privacy Law”, *White & Case*, pp.2-33. [Online]. Available: https://intellicentrics.ca/wp-content/uploads/dlm_uploads/2014/09/article_intldataprotectionandprivacylaw_v5-1.pdf.

Drewitt, T. (2013). “A Manager’s Guide to ISO22301”, *IT Governance Publishing*, pp.11-18 and pp.100-112.

European Parliament. (1995). “Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data”, *Official Journal of the European Communities*, Vol.38, pp.31-50.

European Parliament. (2012). “Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)”, pp. 1-99. [Online]. Available: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.

European Parliament. (2016). “Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of Such Data, and repealing Directive 95/46/EC (General Data Protection Regulation), *Official Journal of the European Communities*, Vol.38, pp.1-88.

Finn, R.L., Wright, D. and Friedewald, M. (2013). “Seven Types of Privacy”, *European Data Protection: Coming of Age*, Springer Netherlands, pp.3-32.

Floor, J. (2015). “No More Data Loss Coverups for SA Businesses”, *Swart Attorneys*. [Online]. Available: http://www.itnewsafrica.com/2015/04/no-more-data-loss-coverups-for-sa-businesses/.

Galvez Cruz, D.C. (2008). “An Environment for Protecting the Privacy of E-Shoppers”, PHD Thesis, University of Glasgow, Scotland, pp.48-52. [Online]. Available: http://theses.gla.ac.uk/590/1/2009Galvezcruzphd.pdf.

Gavison, R. (2012). “Privacy and the Limits of Law”, *The Yale Law Journal*, pp.428-435.

Gawande, A. (2012). “The Checklist Manifesto - How to Get Things Right”, *Business Book Summaries*, p.1. [Online]. Available: http://cdn2.hubspot.net/hub/155473/file-410075999-pdf/Checklist_Manifesto_Doc_(Final).pdf.

Gemalto. (2015). “2015 The Year Data Breaches Got Personal - Findings from the 2015 Breach Level Index”, p.13. [Online]. Available: http://www.gemalto.com/brochures-site/download-site/Documents/ent-Breach_Level_Index_Annual_Report_2015.pdf.

Gerber, M. and Skolmen, D.E. (2015). “Protection of Personal Information in the South African Cloud Computing environment: A Framework for Cloud Computing Adoption”, *2015 Information Security for South Africa (ISSA)*, pp.4-5.

Gormley, K. (1992). “One Hundred Years of Privacy”, *Wisconsin Law Review*, pp.1337-1338.

Government of Argentina. (2000). “Personal Data Protection Act (Act 25)”, pp.1-21. [Online]. Available: http://unpan1.un.org/intradoc/groups/public/documents/un-dpadm/unpan044147.pdf.

Government of Australia. (1988). “Privacy Act (Act 199 of 1988)”, pp.1-258. [Online]. Available: https://www.legislation.gov.au/ComLaw/Legislation/ActCompilation1.nsf/0/D3C265274169345ACA25736E001DB439/$file/Privacy1988_WD02HYP.pdf.

Government of Canada. (2014). “Personal Information Protection and Electronic Document Act (PIPEDA)”, pp.1-47. [Online]. Available: http://laws-lois.justice.gc.ca/PDF/P-8.6.pdf.

Government of Japan. (2003). “Act on the Protection of Personal Information (Act 47 of 2003)”, pp.1-22. [Online]. Available: http://www.cas.go.jp/jp/seisaku/hourei/data/APPI.pdf.

Government of New Zealand. (1993). “Privacy Act (Act 28)”, pp.1-162. [Online]. Available: http://www.legislation.govt.nz/act/public/1993/0028/48.0/096be8ed804c580c.pdf.

Greenleaf, G. (2013). “Research Handbook on Governance of the Internet”, pp.222-225.

Greens, J.P.A. (2015). “EU General Data Protection Regulation State of Play and 10 Main Issues”, p.1. [Online]. Available: http://www.janalbrecht.eu/fileadmin/material/Dokumente/Data_protection_state_of_play_10_points_010715.pdf.

Grobler, M., Irwin, B. and Swart, I. (2014). “On the Viability of Pro-Active Automated PII Breach Detection: A South African Case Study”, *Southern African Institute for Computer Scientist and Information Technologists Annual Conference 2014*, pp.1-8.

Heyink, M. (2015). “A Guide to the Protection of Personal Information Act”, *De Rebus 2015*, p.60. [Online]. Available: http://journals.co.za/docserver/fulltext/derebus/2015/557/derebus_n557_a30.pdf?expires=1486760516&id=id&accname=guest&checksum=359466F71F3E9D29B1C1BBB3BFCFFB10.

Hoar, S.B. (2001). “Identity Theft: The Crime of the New Millennium”, *Oregon Law Review*, Vol.80, No.4, p.1423.

Holvast, J. (2009). “History of Privacy”, *The Future of Identity in the Information Society, Privacy and Identity 2008, IFIP Advances in Information and Communication Technology*, Vol.298, pp.13-40.

Identity Force. (2016). “The Biggest Data Breaches in 2016”. [Online]. Available: https://www.identityforce.com/blog/2016-data-breaches.

Identity Theft Resource Centre. (2016). “2016 Data Breach Category Summary”, p.1. [Online]. Available: http://www.idtheftcenter.org/images/breach/ITRCBreachStatsReportSummary2016.pdf.

Information Is Beautiful. (2017). “World’s Biggest Data Breaches - Selected Losses Greater Than 30000 Records, Updated 5th Jan 2017”. [Online]. Available: http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/.

Information Systems Audit and Control Association (ISACA). (2006). “Information Security Governance: Guidance for Boards of Directors and Executive”, *Second Edition*, pp.7-45.

Information Systems Audit and Control Association (ISACA). (2007). “COBIT 4.1”, *IT Governance Institute*, p.13 and pp.190-192.

Information Systems Audit and Control Association (ISACA). (2009). “The Risk IT Framework”, pp.17-30.

Information Systems Audit and Control Association (ISACA). (2013) “CISA Review Manual 2013”, p.341.

Information Systems Audit and Control Association (ISACA). (2014a). “Risk to Entities Regarding Data Breaches - Lessons from a Brief Case Study”, *Information Systems Audit and Control Association (ISACA) Journal*, Vol.2, p.14.

Information Systems Audit and Control Association (ISACA). (2014b). “CRISC Review Manual 2014”, pp.125-126.

Information Systems Audit and Control Association (ISACA). (2014c) “COBIT 5”, pp.11-88.

International Organisation for Standardisation (ISO). (2012). “ISO 22301:2012: Societal Security - Business Continuity Management Systems - Requirements”, *First Edition*, pp.V-VII and pp.1-23.

International Organisation for Standardisation (ISO). (2013). “ISO/IEC 27001:2013: Information Technology - Security Techniques - Information Security Management Systems - Requirements”, *2013 Edition*, p.V and pp.1-22.

Internet Society. (2016). “Global Internet Report”, pp.8-22 and pp.68-88. [Online]. Available: https://www.internetsociety.org/globalinternetreport/2016/wp-content/uploads/2016/11/ISOC_GIR_2016-v1.pdf.

Javelin. (2016). “2016 Identity Fraud: Fraud Hits an Infection Point”, p.1. [Online]. Available: https://www.javelinstrategy.com/printpdf/23431.

Kanagasingham, P. (2008). “Data Loss Prevention”, *SANS Institute*, p.5. [Online]. Available: https://www.sans.org/reading-room/whitepapers/dlp/data-loss-prevention-32883.

Kirby, M. (2011). “The History, Achievement and Future of the 1980 OECD Guidelines on Privacy”, *International Data Privacy Law*, Vol.1, No.1, p.6.

Kothari, C.R. (2004). “Research Methodology: Methods and Techniques”, *New Age International*, *Second Revised Edition*, p.5.

Kuner, C. (2011). “Regulation of Transborder Data Flows Under Data Protection and Privacy Law: Past, Present and Future”, *OECD Digital Economy Papers*, No.187, pp.10-11.

Kuneva, M. (2009). “Keynote Speech - Roundtable on Online Data Collection, Targeting and Profiling”, p.2. [Online]. Available: http://europa.eu/rapid/press-release_SPEECH-09-156_en.pdf.

Kuschewsky, M. (2014). “The New Privacy Guidelines of the OECD: What Changes for Businesses?”, *Journal of European Competition Law & Practice*, Vol.5, No.3, p.147.

Leard Dissertation. (2012). “Self-Selection Sampling”, *Lund Research Ltd*. [Online]. Available: http://dissertation.laerd.com/self-selection-sampling.php.

Lynch, L. (2013). “EU Data Protection’s Paradigm Shift: From Directive to Regulation”, *Ernst & Young*, p.2. [Online]. Available: http://www.ey.com/Publication/vwLUAssets/EU_Data_Protections_Paradigm_Shift_From_Directive_to_Regulation/$FILE/EU%20Data%20Protections%20Paradigm%20Shift%20From%20Directive%20to%20Regulation.pdf.

Michalsons. (2014). “Protection of Personal Information Act - POPI”. [Online]. Available: http://www.michalsons.co.za/protection-of-personal-information-act-popi/11105.

Michalsons. (2016). “Information Regulator in South Africa”. [Online]. Available: https://www.michalsons.com/blog/information-regulator-in-south-africa/13893.

Milo, D. and Ampofo-Anti, O. (2014). “A Not So Private World”, *Without Prejudice*, Vol.14, Issue 9, pp.30-32.

Monty, S. (2015). “The Popping of POPI”, *Without Prejudice*, Vol.15, Issue 6, pp.86-87.

Moor, J.H. (1997). “Towards a Theory of Privacy in the Information Age”, *ACM SIGCAS Computers and Society*, Vol.27, Issue 3, p.28.

Moore, A.D. (2008). “Defining Privacy”, *Journal of Social Philosophy*, Vol.39, No.3, p.425.

MyBroadBand. (2016a). “Anonymous Hacks Armscor Website”. [Online]. Available: https://mybroadband.co.za/news/security/171505-anonymous-hacks-armscor-website.html.

MyBroadBand. (2016b). “eThekwini Municipality Leaked Private Details of Almost 100000 Residents”. [Online]. Available: https://mybroadband.co.za/news/security/179064-ethekwini-municipality-leaking-private-details-of-over-300000-residents.html.

MyBroadBand. (2016c). “MTN Exposing Subscribers’ Personal Details Online”. [Online]. Available: https://mybroadband.co.za/news/cellular/166734-mtn-exposing-subscribers-personal-details-online.html.

National Crime Prevention Council. (2016). “Evolving with Technology”. [Online]. Available: http://www.ncpc.org/topics/fraud-and-identity-theft/evolving-with-technology.

National Institute of Standards and Technology (NIST). (2009). “Recommended Security Controls for Federal Information Systems and Organisations”, *NIST Special Publication 800-53, Revision 3*, pp.1-238.

National Institute of Standards and Technology (NIST). (2013). “Recommended Security Controls for Federal Information Systems and Organisations”, *NIST Special Publication 800-53, Revision 4*, pp.1-462.

Neethling, J. (2005). “The Concept of Privacy in South African Law”, *The South African Law Journal*, Vol.122, Issue 1, p.19.

Neethling, J, Potgieter, J.M and Visser, P.J. (2005). “Neethling’s Law of Personality”, *Second Edition*, Durban: LexisNexis Butterworths, pp.271-281.

Office of Government Commerce United Kingdom (OGCUK). (2007a). “The Official Introduction to the ITIL Service Lifecycle”, pp.1-170.

Office of Government Commerce United Kingdom (OGCUK). (2007b). “ITIL - Service Design”, pp.65-78 and pp.149-164.

Organisation for Economic Co-operation and Development (OECD). (1980). “OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data - Annex to the Recommendation of the Council of 23 September 1980”, pp.1-4 [Online]. Available: http://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/OECD_Privacy_Guidelines_1980.pdf.

Organisation for Economic Co-operation and Development (OECD). (2009). “Online Identity Theft”, p.16. [Online]. Available: http://www.oecd-ilibrary.org/science-and-technology/online-identity-theft_9789264056596-en.

Organisation for Economic Co-operation and Development (OECD). (2011a). “Thirty Years after the OECD Privacy Guidelines”, p.10. [Online]. Available: http://www.oecd.org/sti/ieconomy/49710223.pdf.

Organisation for Economic Co-operation and Development (OECD). (2011b). “Terms of Reference for the Review of the OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data”, p.3. [Online]. Available: http://www.oecd.org/sti/ieconomy/48975226.pdf.

Organisation for Economic Co-operation and Development (OECD). (2013). “OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data”, pp.1-154. [Online]. Available: http://oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

Organisation for Economic Co-operation and Development (OECD). (2015). “About the OECD”. [Online]. Available: http://www.oecd.org/about/.

Palmer, M.E., Robinson, C., Patilla, J.C and Moser, E.P. (2001). “Information Security Policy Framework: Best Practices for Security Policy in the E-commerce Age”, *Information Systems Security*, Vol.10, Issue 2, p.11.

Parliament of the Republic of South Africa. (2015). “Announcements, Tablings and Committee Reports”, *Cape Town: Government Printer*, No. 70-2015, p.2205.

Perumall, A. (2013). “Problems in Protecting Personal Information”, *Without Prejudice*, Vol.13, Issue 2, pp.61-62.

Privacy International. (2017). “Privacy - Who, What, Why”. [Online]. Available: https://www.privacyinternational.org/.

Reddy, K. (2012). “On Digital Forensic Readiness for Information Privacy Incidents”, PHD Thesis, University of Pretoria, South Africa, pp.10-15. [Online]. Available: http://repository.up.ac.za/bitstream/handle/2263/28209/Complete.pdf?sequence=7.

Rees, M. (2016). “The PoPI Act: Neither Friend Nor Foe - Just Good Business Sense”. [Online]. Available: https://companies.mybroadband.co.za/commvault/2016/11/07/the-popi-act-neither-friend-nor-foe-just-good-business-sense/.

Republic of South Africa. (1996). “Constitution of the Republic of South Africa (Act 108 of 1996)”, *Pretoria: Government Printer*, Issue 32, pp.1249.

Republic of South Africa. (2009). “Protection of Personal Information (POPI) Bill”, *Cape Town and Pretoria: Government Printer*, pp.1-50.

Republic of South Africa. (2013). “Protection of Personal Information (POPI) Act (Act 4 of 2013)”, *Cape Town: Government Printer*, No.37067, pp.2-146.

Roos, A. (2006). “Core Principles of Data Protection Law”, *Comparative and International Law Journal of Southern Africa*, Vol.39, Issue 1, p.130.

Roos, A. (2007). “Data Protection: Explaining the International Backdrop and Evaluating the Current South African Position”, *The South African Law Journal*, Vol.124, Issue 2, p.421-422.

Roos, A. (2016). “Data Protection Law in South Africa”, *African Data Privacy Laws*, Springer International Publishing, pp.3-32.

Saunders, K.M. and Zucker, B. (1999). “Counteracting Identity Fraud in the Information Age: The Identity Theft and Assumption Deterrence Act”, *International Review of Law, Computers & Technology*, Vol.13, No.2, p.183.

Schipke, R.C. (2006). “The Language of Phishing, Pharming, and Other Internet Fraud - Metaphorically Speaking”, *2006 IEEE International Symposium on Technology and Society*, Queens College, Flushing, New York, United States of America, p.1. [Online]. Available: http://ieeexplore.ieee.org/document/4375897/.

Schoeman, F.D. (1984). “Privacy: Philosophical Dimensions”, *American Philosophical Quarterly*, Vol.21, No.3, pp.199.

Sikhungo, M. (2016). “POPI Series - Condition 7 - Information Security”, *Dommisse Attorneys Incorporated*. [Online]. Available: http://dommisseattorneys.co.za/blog/popi-series-condition-7-information-security/.

Solomon, M. (2011). “Using Network Segmentation to Protect the Modern Enterprise Network”, *Security Week*. [Online]. Available: http://www.securityweek.com/using-network-segmentation-protect-modern-enterprise-network.

Solove, D.J. (2002). “Conceptualizing Privacy”, *California Law Review*, Vol.40, Issue 4, Article 2, pp.1099-1124.

Solove, D.J. (2004). “The Digital Person: Technology and Privacy in the Information Age”, *NYU Press*, p.1.

Solove, D.J. (2006). “A Taxonomy of Privacy”, *University of Pennsylvania Law Review formerly American Law Register*, Vol.154, Issue 3, pp.477-479.

Solove, D.J. (2008). “Understanding Privacy”, *Harvard University Press: Cambridge, Massachusetts*, pp.1-7.

Stein, P. (2012). “South Africa’s EU-style Data Protection Law”, *Without Prejudice*, Vol.12, Issue 10, pp.48-49.

Steinke, G. (2002). “Data Privacy Approaches from US and EU Perspectives”, *Telematics and Informatics*, Vol.19, pp.193-200.

Stroud, R.E. (2012). “Introduction to COBIT 5”, p.5. [Online]. Available: http://www.isaca.org/Education/Upcoming-Events/Documents/Intro-COBIT5.pdf.

Symantec. (2016). “2016 Internet Security Threat Report”, p.8. [Online]. Available: https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf

Titus. (2011). “Protecting Personally Identifiable Information (PII) with Classification and Content Inspection”, *Titus White Paper*, p.5. [Online]. Available: http://www.titus.com/resources/marketo/WEB_COM_WP_Protecting_PII.pdf.

United Nations. (1948). “Universal Declaration of Human Rights”. [Online]. Available: http://www.un.org/en/universal-declaration-human-rights/index.html.

United Nations. (1966). “International Covenant on Civil and Political Rights”. [Online]. Available: http://www.ohchr.org/EN/ProfessionalInterest/Pages/CCPR.aspx.

United States Department of Justice. (2015). “Overview of the Privacy Act of 1974 - 2015 Edition”. pp.1-314. [Online]. Available: https://www.justice.gov/opcl/file/793026/download.

United States of America. (1789, 1791 and 1795). “The Constitution of the United States”, pp.11-17. [Online]. Available: http://constitutioncenter.org/media/files/constitution.pdf.

Vermeulen, J. (2016a). “Anonymous Hacks SA Government Database”. *MyBroadBand*. [Online]. Available: https://mybroadband.co.za/news/security/155030-anonymous-hacks-sa-government-database.html.

Vermeulen, J. (2016b). “Anonymous Hacks and Leaks South African Government Data”. *MyBroadBand*. [Online]. Available: https://mybroadband.co.za/news/security/155278-anonymous-hacks-and-leaks-south-african-government-data.html.

World Economic Forum (WEF). (2014). “Global Risks 2014”, *Insight Report, 9th Edition*, pp.12-13. [Online]. Available: http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2014.pdf.

World Economic Forum (WEF). (2015). “Global Risks 2015”, Insight Report, 10th Edition, pp.3-4. [Online]. Available: http://www3.weforum.org/docs/WEF_Global_Risks_2015_Report15.pdf.

World Economic Forum (WEF). (2016). “Global Risks 2016”, Insight Report, 11th Edition, pp.3-5. [Online]. Available: http://www3.weforum.org/docs/Media/TheGlobalRisksReport2016.pdf.

World Economic Forum (WEF). (2017). “Global Risks 2017”, Insight Report, 12th Edition, pp.4-6. [Online]. Available: http://www3.weforum.org/docs/GRR17_Report_web.pdf.