



**Cape Peninsula  
University of Technology**

**Exploring compliance with the protection of Personal Information Act:  
Implementation considerations in small software development companies in  
South Africa**

**by**

**MARVIN WALTER THEYS**

**Thesis submitted in fulfilment of the requirements for the degree**

**MTech: Information Technology**

**in the Faculty of Informatics and Design**

**at the Cape Peninsula University of Technology**

**Supervisor: Prof. Ephias Ruhode  
Co-supervisor: Dr Patricia Harpur**

**Cape Town  
September 2020**

**CPUT copyright information**

The thesis may not be published either in part (in scholarly, scientific or technical journals), or as a whole (as a monograph), unless permission has been obtained from the University

## DECLARATION

### DECLARATION

I, MARVIN WALTER THEYS, declare that the contents of this thesis represent my own unaided work, and that the thesis has not previously been submitted for academic examination towards any qualification. Furthermore, it represents my own opinions and not necessarily those of the Cape Peninsula University of Technology.



Signed

19/07/2020

Date

## ABSTRACT

This study explores the challenges relating to protection of personal information (POPI) compliance within a small software development company. The aim of study is to uncover these challenges and provide guidelines that could assist other small software development companies. Fines of up to ten million rands could be imposed on companies that do not comply. The researcher's experience as a software developer and as an information technology manager, coupled with preliminary studies, revealed that companies have not yet started to prepare for when the Protection of Personal Information Act, No. 4 of 2013 (POPIA) comes into full effect. A review of pertinent literature had themes Consent, Data Officers, Deletion of Personal Information, Policies, and Technical Measures emerge. Consequently, the following research question was formulated, "What implementation guidelines should be considered by SMEs to promote compliance with POPIA?" Two sub-research questions were required to answer the main question. These are Sub-Question 1, "What are current challenges that small and medium enterprises (SMEs) could face when implementing POPIA compliance?" and Sub-Question 2, "How can POPIA compliance implementation challenges be met?" To answer the research questions, the following research design and method were used. A multi-method design was used in an exploratory case study. The methods used in the study incorporate interviews and surveys. Findings suggest that companies will have challenges relating to POPIA compliance. Recommendations include that companies review existing legislative requirements and ascertain if POPIA impacts them in any way, and that staff should receive training on cyber security in the workplace. Furthermore, companies should secure information technology infrastructure, including any software and data, and should have frequent penetration tests conducted by an independent organisation. In addition, company policies should include protection of personal information. Lastly, information technology teams should identify and document threats that could compromise personal information. The study found that POPIA impacts companies subjectively and therefore a recommendation for future research is that similar studies be conducted in various companies to determine the impact POPIA compliance will have. Furthermore, the possibility of an independent body that issues POPIA compliance certificates should be researched.

## ACKNOWLEDGEMENTS

**I wish to thank and acknowledge the following persons and entities:**

- The directors at Medway Marketing and Manage Plus, Mr Lance Allam, Mr Geoff Banwell and Mr Craig Ekermans, for providing me with financial assistance during my MTech studies at CPUT. In addition, I was also granted the privilege of conducting my research at Medway CT.
- The support, guidance, and financial assistance from Mr Rob Rademeyer at Trimble when my MTech studies at CPUT started.
- The directors at 41 Solutions, Mr Rian Fischer and Mr Hendrik Bruwer, for providing me with financial assistance while I was studying towards my BTech degree at CPUT, which I obtained while in their employ (2014 – 2016).
- Golden Arrow Bus Services for providing me with financial assistance while I was studying towards a National Diploma at CPUT, which I obtained while in their employ.
- Prof. Ephias Ruhode, my lecturer at CPUT from 2011 to 2015. Prof. Ruhode became my MTech supervisor in 2018 and would always respond to his students' emails, even when at an airport in Europe. Prof Ruhode is one of the most loved and respected educators at CPUT.
- Dr Patricia-Ann Harpur, my co-supervisor, for her guidance, support, and motivation. We had happy times, sad times and I was even rapped on the knuckles at times. It was a profound journey that we walked together. Her commitment to her students is unquestionable and she is an asset to the academic world.
- Prof. Elizabeth van Aswegen, for editing my work and providing invaluable recommendations.
- The General Manager at Manage Plus, Ms Kathy Maguire, for her profound and invaluable assistance and insight into the business she gave me while conducting my research at work.
- Mr Quinton Williams, for giving me my first software development opportunity in 2013. Thank you, Mr Williams, for welcoming and thrusting me into the world of software development.

- Mrs Soakeyna Martin, for always encouraging me to deliver my best in my personal, academic, and professional life and for being a close family friend since 2013.
- Mr Jason Durbin and Mr Renier Theart for being my rock-solid IT Team.
- Shelby-Anne Theys, my loving wife. Thank you for your rock-solid support throughout my academic career. This would not be possible without the key part that you played.
- Drs Hendrik Theys, for being a great role model, great dad and great grandfather to my sons, Rhiannon, Hayden and Ryan, and to my daughters, Mishkah and Saleen. He is a wonderful father-in-law to my lovely wife, Shelby-Anne Theys, with whom he shares a passion for cooking.
- Simone Stevens (nee Theys), my sister, BCom (UWC) for always having her brother's back and for standing in as our mother, after she left us in 2016, and keeping the family together.
- Mrs Marion Boer (nee Japtha), my mother-in-law, for helping my wife and I when we needed it and for guiding us and strengthening us through prayer.
- Mr Daniel Sydow Theys, for instilling in me a desire to try to achieve my best in life always, to become a better person in all aspects, and to keep learning.
- Mrs Sylvia Heldsinger, for contributing to my work ethic, emphasising the importance of always enjoying one's profession, looking out for others, and sticking to one's commitments.
- Mr Roland and Mrs Katherine Barker for standing in as my parents during my stay in Johannesburg for the period 2006 – 2008.
- Mr Christian Peter Scheffers for being my religious mentor since 2008. Uncle Chris has also been my barber since 1995.
- Ms Annelize for reminding me about the importance of hard work and the sacrifices that need to be made to increase the likelihood of success in any endeavour.
- Mr George Thompson, my uncle, for telling me, "Hard work always wins".
- Mr Earl Julian Theys for recommending that I grow academically. I still have the N+ textbook that he gave me in 2007.
- Ms Lesley-Ann Japtha for motivating me to work harder when pursuing my dreams, irrespective of how tough life gets. One of the quotes most used by her is, "My life isn't rosy, but I make the most of it".

- My best friend, Mr Newton Millan Cloete from UWC. Thank you for standing by me through all the difficult and good times. An academic journey is a never-ending one and I should like to thank you for being there for me since my first year at CPUT.
- Mr Saliegh Aziz from Trimble for being a great role model in the workplace. Mr Aziz always treated everybody with dignity and respect. He is a committed employee of the organisation and a sterling example of what an individual in a leadership position should be.
- 5Ms, my post graduate study group, Mr Thifhuriwi Emmanuel Madzunye, Ms Pinky Motsware, Ms Chiedza Tevera and Mrs Nomputumo Jim. I appreciate the support that I received from the group, the times we got together socially and academically proved to be beneficial both personally and academically.
- Our Heavenly Father, for directing my path for the past 12 years. I would not be capable of achieving what I had without the presence of divinity guiding and keeping me safe.

## DEDICATION

I dedicate this thesis in loving memory of my mother, Susan Mary Theys (nee Thompson). Thank you for always instilling in all your children the importance of having an education and for always being there for every single one of them. Her wish for me in 2008 was that I stop consuming alcohol. This year, 2020, will mark my twelfth year of being alcohol-free. Thank you, Mom.

# TABLE OF CONTENTS

DECLARATION .....	ii
ABSTRACT .....	iii
ACKNOWLEDGEMENTS .....	iv
TABLE OF CONTENTS.....	viii
1 CHAPTER ONE: INTRODUCTION AND OVERVIEW .....	1
1.1 Background to the research problem.....	3
1.2 Problem statement.....	3
1.3 Research questions and objectives .....	4
1.4 Research aim .....	4
1.5 Rationale .....	5
1.6 Delineation of research.....	5
1.7 Contribution of research.....	5
1.8 Ethical considerations.....	5
1.9 Summary .....	6
2 CHAPTER TWO: LITERATURE REVIEW .....	6
2.1 Consent .....	7
2.1.1 Consent: General Data Protection Regulation of the EU.....	7



2.1.2	Consent: Personal Information Protection and Electronic Documents Act of Canada .....	8
2.1.3	Consent: Data Protection Act of Ghana .....	9
2.1.4	Consent: Protection of Personal Information Act .....	9
2.1.5	Crystallization .....	10
2.2	Data officers .....	10
2.2.1	Data Officers: General Data Protection Regulation of the EU .....	10
2.2.2	Data Officers: Personal Information Protection and Electronic Documents Act of Canada.....	11
2.2.3	Data Officers: Data Protection Act of Ghana .....	11
2.2.4	Data Officers: Protection of Personal Information Act.....	11
2.2.5	Crystallisation .....	12
2.3	Deletion of personal information .....	12
2.3.1	Information Deletion: General Data Protection Regulation of the EU.....	12
2.3.2	Information Deletion: Personal Information Protection and Electronic Documents Act of Canada.....	12
2.3.3	Information Deletion: Data Protection Act of Ghana .....	13
2.3.4	Information Deletion: Protection of Personal Information Act .....	13
2.3.5	Crystallisation .....	13
2.4	Policies.....	13

2.4.1	Policies: General Data Protection Regulation of the EU .....	14
2.4.2	Policies: Personal Information Protection and Electronic Documents Act of Canada . .....	14
2.4.3	Policies: Data Protection Act of Ghana .....	14
2.4.4	Policies: Protection of Personal Information Act .....	15
2.4.5	Crystallisation .....	15
2.5	Technical measures.....	15
2.5.1	Technical Measures: General Data Protection Regulation of the EU.....	15
2.5.2	Technical Measures: Personal Information Protection and Electronic Documents Act of Canada.....	16
2.5.3	Technical Measures: Data Protection Act of Ghana .....	16
2.5.4	Technical Measures: Protection of Personal Information Act .....	16
2.5.5	Crystallisation .....	17
2.6	Summary .....	17
3	CHAPTER THREE: RESEARCH DESIGN AND METHODOLOGY.....	19
3.1	Research design.....	19
3.1.1	Philosophies.....	21
3.1.2	Approaches.....	23
3.1.3	Strategies.....	24

3.1.4	Choices .....	25
3.1.5	Time horizons .....	27
3.1.6	Techniques and procedures .....	27
3.1.6.1	Data collection .....	27
3.1.6.2	Interviews.....	27
3.1.6.3	Questionnaire.....	30
3.1.6.4	Data analysis .....	35
3.2	Research methodology .....	36
3.2.1	Sampling.....	36
3.2.2	Data-collection methods.....	39
3.2.3	Case description.....	40
3.2.4	Unit of analysis .....	41
3.2.5	Ethical considerations.....	41
3.2.6	Trustworthiness.....	42
3.2.7	Delimitation.....	44
3.3	Summary .....	45
4	CHAPTER FOUR: FINDINGS AND ANALYSIS.....	46
4.1	Consent .....	48
4.2	Cross-legislation impact .....	49

4.2.1	FAIS Act .....	49
4.2.2	FICA Act .....	50
4.3	Data officers .....	51
4.4	Deletion of personal information .....	53
4.5	Industrial regulatory requirements .....	56
4.6	Information management .....	57
4.6.1	Validation .....	58
4.6.2	Verification .....	58
4.7	Information privacy.....	60
4.8	Policies.....	62
4.9	Reasons for compliance battle .....	64
4.9.1	Archived and backed-up data.....	65
4.9.2	Outdated methods.....	65
4.9.3	Hard copies.....	65
4.9.4	Vague requirements .....	66
4.9.5	Staff and skills training.....	66
4.10	Technical measures.....	71
4.10.1	Hardware protection .....	71

4.10.2	Software protection.....	73
4.11	Summary .....	78
5	CHAPTER FIVE: CONCLUSIONS AND RECOMMENDATIONS .....	81
5.1	Chapter review .....	81
5.1.1	Chapter 1 – Introduction.....	81
5.1.2	Chapter 2 – Literature review .....	81
5.1.3	Chapter 3 – Research design and methodology.....	82
5.1.4	Chapter 4 – Findings and analysis.....	82
5.2	Revisiting the objective and research questions.....	82
5.2.1	What are current challenges that SMEs could face when implementing POPIA compliance (SQ1)?.....	83
5.2.2	How can POPIA compliance implementation challenges be met (SQ2)?.....	86
5.2.3	What implementation guidelines should be considered by SMEs to promote compliance with POPIA (MQ)? .....	90
5.2.4	Summary .....	90
5.3	Limitations of the study .....	92
5.4	Research Contributions.....	92
5.4.1	Theoretical contribution .....	92
5.4.2	Methodological contribution .....	92

5.4.3	Practical contribution.....	92
5.5	Recommendations .....	92
5.5.1	Amend company policy to include POPIA requirements.....	93
5.5.2	Apply security measures to applications and data.....	93
5.5.3	Consider migrating to cloud-based services .....	94
5.5.4	Determine the conflict of requirements between POPIA and other legislation.....	94
5.5.5	Implement the use of digital signatures .....	94
5.5.6	Information systems management teams should identify and document security threats .....	95
5.5.7	Secure information technology hardware infrastructure.....	95
5.5.8	Staff empowerment to include improvement of cyber security awareness .....	96
5.6	Future research.....	97
5.7	Finally .....	97
	REFERENCES.....	98
	LIST OF FIGURES.....	106
	LIST OF TABLES.....	108
	APPENDICES.....	110
	Appendix A – Ethical clearance certificate.....	110
	Appendix B – Interview Protocol .....	111
	Appendix C – Questionnaire C.....	112

Appendix D – Questionnaire A .....	114
Appendix E – Questionnaire B .....	115
Appendix F – Introductory letter for the collection of research data .....	118
Appendix G – Signed consent in principle form .....	119
Appendix H – General manager interview transcript .....	120
Appendix I – Administration manager interview transcript .....	128
Appendix J – IT support technician interview transcript .....	136
Appendix K – Response from the office of the privacy commissioner of Canada .....	141
Appendix L – Codebook.....	142

<b>Abbreviations and Acronyms</b>	
AM	Administration Manager
CMP	Consent Management Platform
DPA	Data Protection Act (Ghana)
DPC	Data Protection Commission
DPO	Data Protection Officer
DPR	Data Protection Register
ECT	Electronic Communications and Transactions Act No. 25 of 2002
EU	European Union
FAIS	Financial Advisory and Intermediary Services Act, No. 37 of 2002
FICA	Financial Intelligence Centre Act, No. 38 of 2001
GDPR	General Data Protection Regulation
GM	General Manager
IS	Information Systems
IT	Information Technology
ITC	TransUnion ITC
ITST	Information Technology Support Technician
PI	Personal Information
PIPEDA	Personal Information Protection and Electronic Documents Act
POPIA	Protection of Personal Information Act, No. 4 of 2013
SME	Small and Medium Enterprise



# 1 CHAPTER ONE: INTRODUCTION AND OVERVIEW

*"When something is important enough, you do it even if the odds are not in your favour" – Elon Musk*

This thesis explores the challenges that SMEs could face when seeking compliance with the Protection of Personal Information Act of South Africa, No. 4 of 2013 (POPIA). In this chapter, the research problem was identified. The research objective and questions were then determined by the research problem.

Small to medium enterprises (SMEs), because of limited resources, struggle to adopt technology (Haseeb et al., 2019). Contrarily, large enterprises are ahead of SMEs in terms of digital trade because of its financial advantage (Robakidze, 2019). The Fourth Industrial Revolution, referred to as Industry 4.0, is changing the way companies compete (Henning, 2019). POPIA compliance may place Information Systems management teams working in SMEs under more strain, both financially and technologically. Strategic IS decisions are needed to secure business value. In the process, tactical managers should be able to control contextual threats. An appropriate set of operational and implementation mechanisms are sought to scaffold ongoing team-player activities. Furthermore, data privacy requirements may impact implementation processes, and consequently IS/IT decision making.

With reference to IS/IT strategy, implementation barriers may manifest in SME enterprises (Noble, 1999). In a recent study, Okumus et al. (2017), identified the IT implementation barriers listed below:

- High costs
- Lack of skills and resources
- Time limitations
- Priority of other businesses
- Technical difficulties
- Internal politics
- Cultural barriers
- Emotions
- Commitment to current practices
- Strong organisational culture

These factors relate easily to the imminent, compulsory adherence to POPIA associated with South African SME projects.

Required within an organisation is an organisation-wide action plan, coupled with a distinct strategy, aiming to address the effectiveness of information dissemination (Chaffey & Wood, 2005). This comment is of significance where SMEs are required to implement measures that protect data privacy.

Furthermore, data protection is a very prevalent conversation worldwide (Wagner & Frank, 2018). South Africa has acted in accordance with world standards regarding the protection or safeguarding of personal or sensitive information of an individual. This was achieved after the POPIA was signed into law by the South African president in November 2013 (Swartz & Da Veiga, 2016). POPIA was published for the first time in the *Government Gazette* in the same month and year. POPIA has gained traction over the last three years as the Information Regulator was officially appointed in 2016 (Burger-Smidt, 2016). The Regulations of POPIA were published in December 2018. A one-year grace period to comply with POPIA, starting from the date that the Act comes into full effect, will be granted to companies (Buys, 2018). Fines imposed for non-compliance could be as high as ten million rands.

The purpose or resolution of POPIA is enforcement of the protection or safeguarding of personal or private information. This relates to information processed by either a public or private body. Furthermore, POPIA must establish requirements for secure processing or handling of information. One of the mandates of POPIA is to establish an Information Regulator who deals with complaints and related matters.

Personal information is defined in POPIA as information that relates specifically to an identifiable, existing, individual. In December 2018, the first revision of the Regulations of POPIA was published by the Information Regulator (Bracher, 2018).

Processing, as defined by POPIA, is any operation, set of operations, activity or set of activities that involve personal information. These activities could be, but are not limited to, the collection and storage of such information or retrieval of this information.

Collectively, when computers are used to retrieve, store, manipulate and transmit data, it is referred to as Information Technology (Daintith, 2009). Processing, as defined by POPIA, is any operation, set of operations, activity or set of activities that involve personal information.

Therefore, when IT is utilised to process personal information, the regulations of POPIA will impact IT directly.

An information systems matrix comprises four IT infrastructure considerations, namely, hardware, software, networking, and data (Pearlson et al., 2019). This matrix informs strategic yet necessary decision making. The legislated implementation of the POPIA Act considers these four facets.

## **1.1 Background to the research problem**

The researcher's experience as a software developer and as an IT manager, coupled with preliminary studies, revealed that companies have not yet started to prepare for POPIA's full implementation. The researcher found that at both micro and macro levels of companies, employees were not even aware that POPIA exists. Macro levels of these companies lacked an understanding of compliance with POPIA as well as the implications of non-compliance. South Africa's ranking in terms of cyber-attack vulnerability is amongst the highest in Africa (Abiodun, Anderson, & Christoffels, 2020). Public and private companies should adhere to data protection legislation as security awareness levels and expectations from individuals are high (Da Veiga & Ophoff, 2020).

## **1.2 Problem statement**

Many SMEs have not commenced preparation for POPIA compliance. Furthermore, these companies might not be aware of the guidelines for successful implementation of POPIA, leading to compliance with the imminent implementation of the POPIA Act. This lack of awareness may impact the functioning of SMEs, leading to costly financial and legal implications. POPIA impacts IT within an SME and the scope of this impact is unknown. The act came into effect July 2020 and companies have until July 2021 to become compliant. SMEs have a responsibility to ensure that personal information is protected. POPIA guides compliance but it impacts companies subjectively.

A gap exists in the literature relevant to POPIA implementation guidelines. A search for practical guidelines yielded little to no results. However, the impact of POPIA on various sectors does offer more literature. The authority of the Information Regulator will require adherence by healthcare practitioners and a call was made to the HPCSA to provide guidelines on dissemination of personal information (Van Niekerk, 2019). Employers can face

dire consequences if POPIA is not implemented (Larsen, 2019). This study offers a set of implementation guidelines that can offer a guide for POPIA compliance.

### 1.3 Research questions and objectives

The problem statement was the basis for the research questions and objectives. These are listed below in Table 1.1.

**Table 1.1 Research questions and objectives**

<b>Research Questions</b>	<b>Objectives</b>
<b>MQ</b> What implementation guidelines should be considered by SMEs to promote compliance with POPIA?	<b>MO</b> Explore implementation guidelines that can be utilized by SMEs that can promote compliance to POPIA.
<b>SQ1</b> What are current challenges that SMEs could face when implementing POPIA compliance?	<b>O1</b> Explore what challenges SMEs could be faced with when implementing POPIA compliance.
<b>SQ2</b> How can POPIA compliance implementation challenges be met?	<b>O2</b> Explore how POPIA implementation challenges can be met.

In the table above, the link between the secondary research questions and objectives is displayed. In column 1, the research questions are presented, and in column 2, the corresponding objectives are presented.

### 1.4 Research aim

The study aims to explore implementation considerations that promote compliance with POPIA within an SME context that utilises IT to meet its business needs, and which includes the software development aspect of IT. The intention is to offer a set of recommendations on how to achieve compliance from an IT and SME perspective. Additionally, the study provides other SMEs with an opportunity to gain insight in POPIA compliance that can assist with the planning of compliance implementation.

## **1.5 Rationale**

Compliance with POPIA should not be taken lightly, as fines of up to ten million rands can be imposed with the possibility of imprisonment. Compliance with POPIA can have a considerable impact on a business and preparations should be made. POPIA is vague about its implementation, which indicates a gap. The research is therefore imperative because it provides insight into actual implementation considerations.

## **1.6 Delineation of research**

The delineation of the research is as follows:

- The researcher is not a legal expert.
- POPIA laws have not been implemented at the company that is part of the research.
- The research will be conducted at a single company within the Western Cape.
- The research focuses on themes that emerged from the literature review only.
- The study excludes sections of POPIA that are not relevant to the themes that emerged from the literature review.

## **1.7 Contribution of research**

The research contributes scientifically to the body of knowledge regarding data protection in South Africa. Furthermore, the study demonstrates methodological facets of case study strategy in the field of information security and data protection. Lastly, the study offers practical recommendations or guidelines that can be utilised by other companies in terms of POPIA compliance.

## **1.8 Ethical considerations**

The potential for physical, psychological, social, cultural, or financial harm to participants not directly involved in the study is unlikely. Respondents in the interviews as well as those who participated in the survey were given the choice of remaining anonymous. Respondents were informed that they could choose to cancel the interview at any time. Similarly, respondents presented with the questionnaire were informed that they could withdraw at any time. The company granted the researcher the right to conduct research on the premises and with employees. CPUT issued an ethical clearance certificate to conduct the research.

## 1.9 Summary

In summary, the problem statement, research objective and questions, research aim, and rationale were outlined. In the next chapter, literature relevant to the study is reviewed.

## 2 CHAPTER TWO: LITERATURE REVIEW

*“We will only master challenges of our time if we stand united and work together with others across borders” – Angela Merkel*

In the previous chapter, the research problem and research questions were presented. In this chapter, the literature review is presented.

Striving towards POPIA compliance within an organisation warrants the consideration of certain factors. It is a new law aimed at data protection in South Africa, whereas other countries have had this type of law in place since as early as the late 1980s. As a recommendation, South Africans should take similar routes that other countries have followed in terms of privacy Act compliance processes (Botha, Eloff, & Swart, 2014). To inform the study, data protection laws and challenges resulting from compliance in other countries are explored. In addition to a review of POPIA, considered compliance regulations that inform this study include the following:

- General Data Protection Regulation of the EU (GDPR).
- Personal Information Protection and Electronic Documents Act of Canada (PIPEDA).
- Data Protection Act of Ghana (DPA).

The GDPR, based on the fundamental human right to privacy, has a global reach (Goddard, 2017). It was therefore decided to include the GDPR as part of this study. PIPEDA has been enacted in 2000 and has evolved over time (O'Donnell, 2020). PIPEDA has a history of refinement over time and has therefore been included as part of this study. In 2011, Ghana was considered as a cyber-crime hub (Warner, 2011). Therefore, the DPA has been included as part of this study.

In addition to data protection regulation compliance, companies need to ensure that security implementations remain monitored, controlled, and audited (Hallová et al., 2019). This means that data security is not a once off exercise, but rather a continuous process. In a study relating

to the GDPR, the term “data trust” refers to a combination of aspects made up of organizational structure, technical and legal expertise (Stalla-Bourdillon et al., 2020). This means that data protection is a process that involves multiple role players, with distinct sets of expertise, to be effective. A result of SMEs reducing their budget for IT security has seen an increased exposure to various threats (Rubio, Chavarria & Mauricio, 2020). SMEs should consider security as an important investment.

Factors promoting compliance with POPIA are identified in this section. The main themes that have emerged from this study are:

- Consent (Section 2.1)
- Data officers (Section 2.2)
- Deletion of personal information (Section 2.3)
- Policies (Section 2.4)
- Technical measures (Section 2.5)

Each of these themes is discussed relative to GDPR, PIPEDA, DPA, and POPIA. This preliminary literature review section closes with Section 2.6, which provides a crystallisation of Sections 2.1 – 2.5.

## **2.1 Consent**

Sections 2.1.1 – 2.1.4 examine consent as requirements of the GDPR, PIPEDA, DPA, and POPIA. A summary is provided in Section 2.1.5.

### **2.1.1 Consent: General Data Protection Regulation of the EU**

According to GDPR Recital 32, consent is required from an individual when data is sent to any third country. Processing the data of an individual requires consent be given freely by the subject in the form of written consent, electronic means or ticking boxes from websites. GDPR Recital 32 states that consent will not however be considered lawful if the user gives consent with pre-ticked tick boxes on websites. Recital 33 of the GDPR states that consent should be granted by the data subject if the data will be used in certain types of research. GDPR Recital 38 stipulates that parental consent is not required when offering services such as counselling or preventative services directly to a child. GDPR Recital 40 states that processing will only

be considered lawful on the basis that consent from the data subject has been granted or some other legitimate basis. It is therefore evident that consent is considered an important factor when dealing with personal information, so important that it warrants specific regulations. The strict regulations posed by the GDPR surrounding consent, specifically revoking consent, did however have a negative effect on research, researchers and research results in the EU (Politou et al., 2018). More than half of the famous European websites have displayed consent notices since the adoption of the GDPR (Utz et al., 2019). Website owners in the EU make use of consent management platforms to assist with regulatory compliance, focusing specifically on consent (Nouwens et al., 2020). Under the GDPR, withdrawal of consent has left businesses with the challenge of having to be able to remove data upon receipt of such a request (Debruyne et al., 2020). Furthermore, such information could exist within a distributed system.

### **2.1.2 Consent: Personal Information Protection and Electronic Documents Act of Canada**

PIPEDA states that knowledge and consent are required for processing personal information, except in certain circumstance, for legal, medical or security reasons where seeking consent would be impossible or impractical. Consent is required for the collection of personal information and in certain circumstances consent may be sought after collection but before use. When consent is sought, companies must ensure that the data subject is completely aware of the nature of the information use or disclosure. An organisation shall not require consent of the data subject for purposes other than what is required as is explicitly specified and legitimately required. The type of consent sought by an organisation may vary, depending on circumstances and type of information or level of sensitivity; an example of such information would be medical records which could almost certainly be sensitive. The regulations regarding consent to disclosure of medical information of an individual have posed Canadian researchers with a wide array of issues, most of which have resulted in cancellation of studies, increased tuition fees and a decrease in recruitment (Harris, Levy, & Teschke, 2008). PIPEDA's consent regulations should be strengthened and not relaxed to accommodate the current advances in terms of technology, economy and social developments (Trosow et al., 2016). The Office of the Privacy Commissioner of Canada confirmed that they do grant individuals permission to withdraw consent (see Appendix K).



### **2.1.3 Consent: Data Protection Act of Ghana**

In the section Consent, justification, and objection of DPA, it is clearly stated that data will not be collected from a data subject unless consent is given. A challenge faced in Ghana with relation to data privacy is the lack of understanding of the general population (Agyei-Bekoe, 2013). This might cause difficulties for companies regarding obtaining consent. Ghana has been recognised as a major hub of cyber-criminal activity (Warner, 2011). This could contribute to people's reluctance to provide consent for processing of their information. Online fraud committed in Ghana resulted in Ghana's ban from e-commerce (Guermazi & Satola, 2005). This could have created a rise in mistrust levels among the general population of Ghana in respect of providing consent for information processing.

### **2.1.4 Consent: Protection of Personal Information Act**

The section in POPIA entitled "Consent, justification and objection" states that processing of personal information requires consent when the data subject is a child and consent has been granted by an adult (South African Government, 2013). Furthermore, the responsible party that processes the information of the child data subject should be able to prove that consent has been granted. Consent is not required when processing a data subject's information when it is required for fulfilling contractual obligations. The Regulations of POPIA only offer implementation guidelines surrounding consent in respect of direct marketing by electronic communication where it explicitly states that only written consent will be considered lawful. Therefore, one can assume that consent in any form for legitimate processing of personal information, other than direct marketing, will be accepted and considered lawful. This is good news for businesses that are already processing personal information because direct marketing companies will be affected mostly by this. The bad news for some companies is that they will have to (if no consent has been granted by the data subjects in writing) remove all personal data that they have received without written consent for marketing purposes or request consent in writing from all the data subjects in question. POPIA does however state clearly that it does not need consent for matters relating to the law. In a related study an experiment was conducted to determine the flow of personal information, by using new email addresses and Cellphone numbers, between insurance companies (Zenda, Vorster, & Viegas, 2020). The results indicated that 92% of marketing communication was received from insurance companies that were not part of the experiment.

### **2.1.5 Crystallization**

It is evident, when comparing the privacy laws of different countries, that legal authorities have the right to process the personal information of a data subject stored by any party and consent is therefore not an absolute prerequisite. It is evident that consent is of pivotal importance when it comes to data privacy, some regulations being more specific than others. In terms of implementation of consent mechanisms in South African businesses, the only real challenge is to companies that use personal data for direct marketing purposes. These companies should be able to remove the information when consent is withdrawn.

## **2.2 Data officers**

Sections 2.2.1 – 2.2.4 provide an examination of the designation of data officers as requirements from the GDPR, PIPEDA, DPA, and POPIA. A summary is provided in Section 2.2.5.

### **2.2.1 Data Officers: General Data Protection Regulation of the EU**

The GDPR in Article 37–39 covers the requirements of a data protection officer (DPO). Article 37 states that a processor or controller shall designate a DPO where the processing is carried out by an organisation, except for courts in their judicial capacity, where the data processed is done on a large scale and when information processing involves personal data relating to criminal convictions and offences. It states that a group of companies can appoint a single DPO provided that the officer is easily. Article 37 further sets out the provisions relating to the appointment of a DPO, all of which will not be mentioned in this study. Article 39 outlines the tasks that a data protection officer shall undertake. The DPO will inform and advise the controllers and their employees based on the GDPR, and monitor compliance with the GDPR, including the delegation of responsibility, awareness raising and training of staff involved in processing operations and related audits. The DPO will, in addition to the tasks, cooperate with the supervisory authority, and act as a point of contact for the supervisory authority about any issues concerning data privacy. Lastly, the DPO shall, in the performance of his or her duty, remain cognisant of risks involved in the specific processing operations. DPOs are the main responsible parties handling compliance with the GDPR within companies (Boban, 2016). DPOs are important within companies (Chassang, 2017).

### **2.2.2 Data Officers: Personal Information Protection and Electronic Documents Act of Canada**

The Canadian federal government decided to follow the European lead, enact a privacy statute for the private sector, and give responsibility for oversight to the Office of the Privacy Commissioner of Canada (Bennett, Regan, & Bayley, 2017). PIPEDA does not require the designation of a data protection officer, as contraventions of the Act will be dealt with directly by the Privacy Commissioner. The Privacy Commissioner deals with PIPEDA complaints in most of Canada (Bennett et al., 2017).

### **2.2.3 Data Officers: Data Protection Act of Ghana**

The DPA, like PIPEDA, does not require the designation of a data protection officer or information officer. The Data Protection Commission investigates all data privacy complaints, monitors compliance, regulates the processing of personal information and maintains the Data Protection Register. The purpose of the Data Protection Register is to keep a record of all data controllers and maintained by the DPC. All data controllers shall register with the DPC.

### **2.2.4 Data Officers: Protection of Personal Information Act**

POPIA states in Part B, Information Officer, Designation and Delegation of Deputy Information Officers, Section 56, that any public and private body should designate an information officer and, in some instances, even deputy information officers (South African Government, 2013). Section 55 of the Act provides a description of the five duties and responsibilities required to be performed by an information officer. First is to encourage compliance with POPIA in the body's data-processing activities. Second is to handle POPIA-related queries or requests. Third is to work together with the Information Regulator when investigations are carried out regarding complaints. Fourth is ensuring POPIA compliance within the organisation. Last is to perform any duty as prescribed by the Act. Information officers must be registered with the Information Regulator before commencing their duties. The objectives of competition and data protection law overlap, and through cooperation between the Information Regulator and the Competition Commission, they could address issues more effectively and efficiently (Koornhof & Pistorius, 2018). Therefore, when implementing the appointment of an Information Officer within a public or private body that conducts business that falls within the ambit of another Act that impacts that business, preference should be given to individuals or entities that have

experience in this field and that understand the workings of the company and its commitments under the other Act that governs its functions.

### **2.2.5 Crystallisation**

The appointment of data officers is not standard across the data laws examined, as only the GDPR and POPIA require this. These officers are the link between the supervisory authorities and the complainants. Their role is crucial, as they need to ensure compliance with the regulations. Industry-specific data officers should be considered, as they could enhance the efficiency of interaction between the Information Regulator and data processors. Therefore, the designation of an information officer is an important consideration.

## **2.3 Deletion of personal information**

Sections 2.3.1 – 2.3.4 present an examination of the right to have data deleted as required by the GDPR, PIPEDA, DPA, and POPIA. A summary is provided in Section 2.3.5.

### **2.3.1 Information Deletion: General Data Protection Regulation of the EU**

Article 17 in the GDPR grants an individual the right to have personal information removed. The data controller, which can mean the company or entity that has the information, should act on the request of an individual to have their information removed by means that are not overly excessive, considering the costs and available technologies, and should inform any other data controllers with whom it has shared the information to delete it. Google had to remove the personal information of an individual, Mario Costeja González, from its search results as this was historical information and could negatively affect the individual (Watanabe, 2016). Google has faced quite few legal battles regarding personal information and its deletion (Kampmark, 2015).

### **2.3.2 Information Deletion: Personal Information Protection and Electronic Documents Act of Canada**

Although PIPEDA does not explicitly grant the “right to deletion” as with the GDPR and POPIA, it does however require, in Section 4.5.3, that information be erased, anonymised or destroyed when the information is no longer required to fulfil the initial need thereof and when consent is withdrawn. Thus, according to PIPEDA, users do not request to have their data removed; they need to withdraw consent.

### **2.3.3 Information Deletion: Data Protection Act of Ghana**

The DPA covers the deletion of information regarding retention of records. It grants the right to an individual to have his or her information removed when it is inaccurate, out of date, obtained in an unlawful manner, or if the information is irrelevant, incomplete or misleading under the section 'Correction of personal data', and compels the data controller to either delete or destroy the data.

### **2.3.4 Information Deletion: Protection of Personal Information Act**

In the section "Correction of personal information", POPIA grants the right to an individual to request that their information be deleted (South African Government, 2013). POPIA requires the deletion of personal information when data retention is no longer required.

### **2.3.5 Crystallisation**

Deletion of personal information can have a considerable impact on companies (Kampmark, 2015). The GDPR, DPA, and POPIA make specific reference to deletion of records in terms of users' requesting deletion of information. PIPEDA, although it does not cater specifically to requests for the deletion of records, does enforce deletion in terms of retention and when an individual withdraws consent. POPIA requires deletion under certain circumstances. Therefore, the right to deletion and retention of records is an important factor to be considered when seeking POPIA compliance. Companies need to determine the extent to which deletion is possible, and if personal information is propagated, a record must be kept and the propagated data should be kept up to date also.

## **2.4 Policies**

Sections 2.4.1 – 2.4.4 present an examination of the implementation or adoption of internal policies as requirements from the GDPR, PIPEDA, DPA, and POPIA. Section 2.4.5 provides a summary.

### **2.4.1 Policies: General Data Protection Regulation of the EU**

Recital 78 of the GDPR requires the adoption of internal policies by data controllers to ensure that the principles of data protection by design and data protection by default are met. It further states the right to data protection and compliance with the GDPR must be considered when acquiring or using applications, services or products. This simply means, for example, that if a company chooses to use an external company to develop software, this company must develop it in such a way that it is compliant with GDPR. This is done to prevent putting the client at risk of being non-compliant. They do not provide strict methods on how to draft policies, because of the reasonable assumption that businesses have different procedures and software products designed to meet specific business goals. Facebook had to update its privacy policies after the Cambridge Analytica incident in accordance with the GDPR's policy requirements (Shvartzshnaider et. al., 2018). Facebook prioritises the security of its users' information and takes compliance with the GDPR very seriously (Facebook, 2018).

### **2.4.2 Policies: Personal Information Protection and Electronic Documents Act of Canada**

PIPEDA, in Section 4.1.4, requires the implementation of policies and practices, which include the implementation of procedures to protect PI, procedures to receive and respond to complaints and enquiries, training staff, communicating to staff information about the organisation's policies and practices, and developing information to explain the organisation's policies and procedures. Section 4.4.1 prohibits the collection of PI that is not required by the data controller. Furthermore, it states that the organisation shall specify the type of information collected as part of their information-handling policies and practices in accordance with the openness principle in Section 4.8. It states that an organisation will avail to individuals, specific information about its policies and practices relating to the management of PI. Application users typically do not read privacy policy or terms of use documents (Trosow et al., 2016). Irrespective of this, policies are still required.

### **2.4.3 Policies: Data Protection Act of Ghana**

Section 28, Security Measures, states that organisational measures be put in place to protect PI. It does not state anything specifically relating to policies within an organisation. One can thus assume that reasonable organisational measures could refer to the drafting of internal policies.

#### **2.4.4 Policies: Protection of Personal Information Act**

POPIA does not explicitly state the requirements for policies that companies need to put in place. A reasonable assumption is that policies are alluded to in Condition 7: Security and Safeguards, where it states that a responsible party must secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate organisational measures to prevent loss or damage to or unauthorised destruction of PI and unlawful access to or processing of personal information (South African Government, 2013). Health research will be impacted by POPIA even though it is currently regulated by the Constitution (Staunton et al., 2020). The Apple Watch privacy policy was found to be compliant with POPIA (Katurura & Cilliers, 2019). It was recommended that certain provision be made in POPIA to promote the digitization of agriculture in South Africa (Aguera et al., 2020). It is evident that POPIA affects different industries and therefore warrants the drafting or creating of industry and purpose specific data protection policies.

#### **2.4.5 Crystallisation**

The GDPR and PIPEDA do not leave any room for misinterpretation in respect of the importance of the creation and adoption of policies within companies. It is of some concern that POPIA and DPA do, however, fail to mention the adoption or creation of policies explicitly within companies which seek to promote the protection of PI. Therefore, when implementing POPIA, one should consider the adoption and creation of internal policies with the aim of protecting information. Internal policies will be organisation specific.

### **2.5 Technical measures**

Technical measures refer to the electronic sphere of data protection. Sections 2.5.1 – 2.5.4 provide an examination of technical measures from the GDPR, PIPEDA, DPA and POPIA. A crystallisation is given in Section 2.5.5.

#### **2.5.1 Technical Measures: General Data Protection Regulation of the EU**

The GDPR recommends the use of pseudonymisation in GDPR Article 25, titled, “Data protection by design and by default”. Pseudonymisation is a method used to increase the level of information privacy of individuals when their data is collected or processed (Zimmer, Burkert, Petersen, & Federrath, 2020). This technique, if not implemented correctly, can be susceptible to attack and therefore more advanced applications of this technique should be

applied (Smith, 2017). The GDPR recommends that data be encrypted in GDPR Article 32. Encryption is called encipherment, which is the process of disguising information as 'ciphertext' or rendering data unintelligible to an unauthorised person.

### **2.5.2 Technical Measures: Personal Information Protection and Electronic Documents Act of Canada**

Although it does not prescribe a specific technology for securing information, it does have a set of conditions that must be met for an electronic signature to be considered valid [Article 48(1) and (2)]. PIPEDA in Part 2, Electronic Documents, defines an electronic signature as “a signature that consists of one or more letters, characters, numbers or other symbols in digital form incorporated in, attached to or associated with an electronic document”. Electronic signatures, known as digital signatures, are a method of encryption where the sender encrypts the message using a private encryption key. The receiver then decrypts the message using a public key of the sender, thus ensuring that the message came from the sender (Chaum, 1992).

### **2.5.3 Technical Measures: Data Protection Act of Ghana**

The DPA, in Section 28, makes provision for data security. Although it does not prescribe a specific technology, it states that reasonable technological methods be implemented, and these measures should be constantly improved.

### **2.5.4 Technical Measures: Protection of Personal Information Act**

The Regulations of POPIA defines an electronic signature as defined in the Electronic Communications and Transactions Act No. 25 of 2002. It defines an advanced electronic signature as “an electronic signature which results from a process which has been accredited by the Authority as provided for in section 37”. POPIA or the regulation does not prescribe the use of any specific technology (South African Government, 2013). POPIA states in Condition 7 that, “A responsible party must secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures to prevent loss of, damage to or unauthorised destruction of personal information; and unlawful access to or processing of personal information”. A practical guideline to enforce POPIA compliance from a data management perspective is possible but providing a standard for data management will require input from a collection of data management professionals (Kandeh, Botha, & Fitcher, 2018).



### **2.5.5 Crystallisation**

Encryption is mentioned in GDPR and PIPEDA and can therefore be considered a reasonable security safeguard mechanism. Encryption, used as a security measure, promotes the confidentiality of data and communication (Oberholzer, 2001). The DPA and POPIA state that reasonable measures be put in place without any specific guidelines as to how these will be achieved. It can therefore be deduced that the type of technical safeguards implemented are at the discretion of the data processor, as no regulation exists in this regard in POPIA. In a healthcare context, it has been found that although companies implement technical security measures, if users act in a careless manner, their actions could defeat the purpose of the security measures put in place (Box & Pottas, 2014). Therefore, a company can determine whether its technical implementations are of a high standard or adequate. Technical measures are not an absolute protection mechanism, as risky behaviour by users could compromise them. Software developers should, as a rule, consider the implementation of security concepts as a standard that should be strictly adhered to.

## **2.6 Summary**

In summary, the GDPR is an almost exhaustive data protection regulation when compared with the PIPEDA, DPA (Ghana) and POPIA in terms of policies, technical measures, consent, and data officers. The GDPR mentions specific technical measures like pseudonymisation and encryption, PIPEDA mentions encryption, whereas the DPA and POPIA do not. The GDPR, along with PIPEDA, specifically requires that internal privacy policies be drafted, whereas the DPA and POPIA do not. All the data laws stress the importance of consent. The GDPR goes so far as to recognise and regulate consent given via websites. The GDPR and POPIA do require the appointment of data officers, whereas the PIPEDA and DPA do not. This is a responsibility of the information officer in terms of POPIA. Table 2.1 overleaf compares differing data protection provisions

**Table 2.1 Comparison of different data protection laws**

	Policies	Technical measures	Consent	Data officers	Deletion of information
GDPR	X	X	X	X	X
PIPEDA	X	X	X		X
DPA			X		X
POPIA			X	X	X

Table 2.1 above summarises the outcome of the initial literature review, indicating five emergent themes. Additionally, the zones shaded red illustrate thematic gaps. The POPIA in South Africa is not specific in terms of policies and technical measures.

In closing, the research questions and objectives remain valid. For the convenience of the reader, Table 1.1 is repeated here as Table 2.2.

**Table 2.2 Research questions and objectives**

Research Questions	Objectives
<b>MQ</b> What implementation guidelines should be considered by SMEs to promote compliance with POPIA?	<b>MO</b> Explore implementation guidelines that can be utilized by SMEs that can promote compliance to POPIA.
<b>SQ1</b> What are current challenges that SMEs could face when implementing POPIA compliance?	<b>O1</b> Explore what challenges SMEs could be faced with when implementing POPIA compliance.
<b>SQ2</b> How can POPIA compliance implementation challenges be met?	<b>O2</b> Explore how POPIA implementation challenges can be met.

Therefore, the research questions remain valid. In the next chapter, the research design and methodology are reviewed.

### 3 CHAPTER THREE: RESEARCH DESIGN AND METHODOLOGY

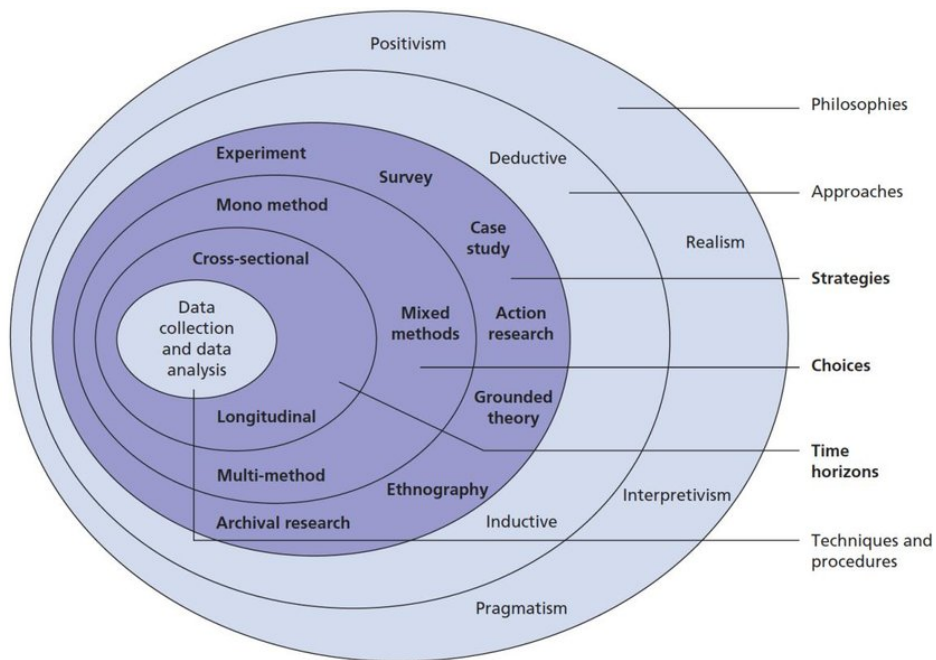
*“The writing of a melody is an emotional moment; success doesn’t make it easy” – Eithne Pádraigín Ní Bhraonáin (Enya)*

In Chapter 2, a literature review informed the study in respect of different aspects addressed by data protection regulations and Acts globally. The review highlighted differences between POPIA and other data laws. The aspects reviewed were policies, technical measures, consent, data officers, and deletion of personal information. The review highlighted requirements of POPIA that South African businesses need to adhere to. Businesses in South Africa that would be impacted most would be marketing businesses, as they require written consent.

In this chapter, the research design and methodology underpinning the study are discussed. Sections are split into two: Research Design, and Research Methodology. Research design (Section 3.1) refers to the planning of the design and providing the rationale for the chosen design. Research methodology (Section 3.2) refers to how the research was conducted. The chapter closes with a summary in Section 3.3.

#### 3.1 Research design

The research design follows the model as adopted from the research onion (Saunders, Lewis, & Thornhill, 2012).

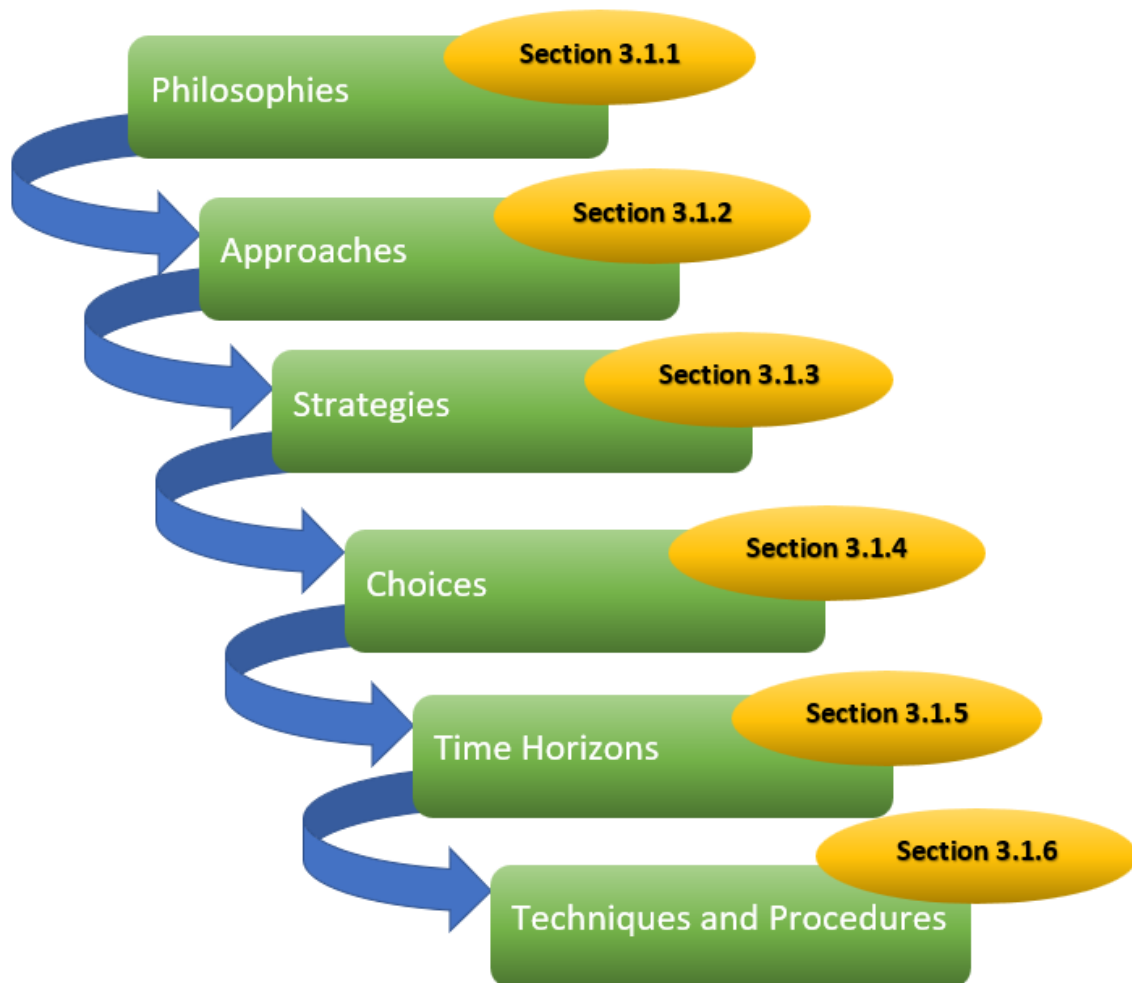


**Figure 3.1 - The research onion (Saunders et al. 2012:108)**

The sections below contain discussions on the following topics in the order that they appear in the research onion:

- Philosophies (3.1.1)
- Approaches (3.1.2)
- Strategies (3.1.4)
- Choices (3.1.3)
- Time horizons (3.1.5)
- Techniques and procedures (3.1.6)

In accordance with the research onion, these topics need to follow a sequence, but could be iterative, as depicted in the diagram below.



**Figure 3.2 Research design**

The first topic discussed in the next section is philosophies.

### **3.1.1 Philosophies**

Research philosophy forms the basis for research and guides the researcher's choice of the research strategy, construction of the problem, data collection, preparing the data, and data analysis (Žukauskas, Vveinhardt, & Andriukaitienė, 2018). A paradigm is a worldview or basic set of rules and beliefs that directs research (Guba & Lincoln, 1994). Therefore, the philosophy

or paradigm provides the researcher with a set of guidelines or beliefs that should be followed as an important part of any scientific research as it impacts the research holistically.

Ontology and epistemology impact sampling techniques employed (Uprichard, 2013). This means that ontological and epistemological foundations that exist as part of a study will guide the sampling technique chosen by the researcher.

**Ontology** is the questioning of reality and whether an objective reality can exist that is not dependent on the researcher (Creswell, 1994). A positivist ontology is defined as naïve realism. The positivist believes the interpretation of the world should be done objectively as this is the only way to uncover true knowledge (Lincoln & Guba, 2005). In addition, some constructivists believe that meaning is of importance, maybe more so meaning-making, as phenomena can be the result of meaning-making within a certain group of people. Ontologically, interpretivism is best labelled as constructivism (Goldkhul, 2012). Constructivists often adopt a subjective view of knowledge (Lincoln & Guba, 2000).

**Epistemology** pertains to the source and nature of true knowledge, the ability of research subjects to possess knowledge, and to theories of knowledge (Childers & Hentzi, 1995). This means that positivists believe that the world can be interpreted in a singular manner. Interpretivists hold the belief that knowledge is subjective, based on individual experiences and not generalisable (Hiller, 2016). This means that knowledge is not absolute and differs between individuals and experiences. Therefore, interpretivists believe in a reality that is subjective.

In summary, O'Leary (2017) groups the research paradigms, positivism and interpretivism, as quantitative and qualitative methods, respectively. This means that positivist research would make use of methods that are consistent with quantitative research. Interpretivism, on the other hand, would make use of qualitative research methods.

In Table 3.1 below, the first column contains the differences highlighted in the previous sections. Row 1 contains the research philosophies. The table displays the differences between the two philosophies.

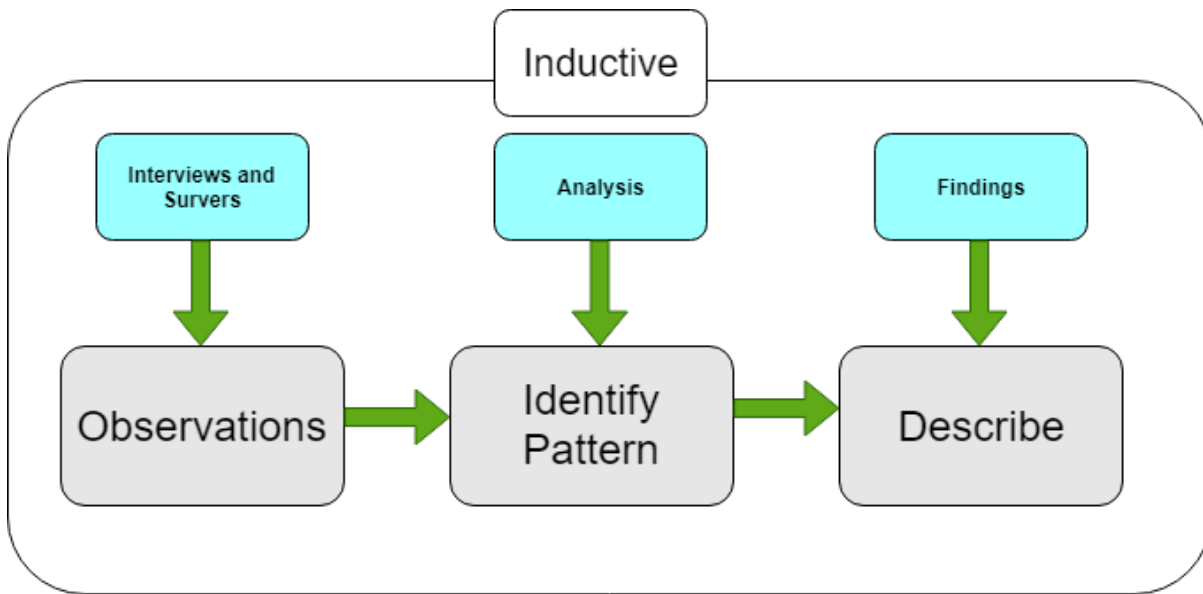
**Table 3.1 Philosophy comparison**

	<b>Positivism</b>	<b>Interpretivism</b>
<b>Methodological Paradigm</b>	Quantitative (O’Leary, 2017)	Qualitative (O’Leary, 2017)
<b>Ontology</b>	Naive realism (Lincoln & Guba, 2005)	Constructivism (Goldkhal, 2012)
<b>Epistemology</b>	Singular reality (Kaptizke, 2003)	Subjective reality (Hiller, 2016)

The philosophy underpinning this study was interpretivism.

### **3.1.2 Approaches**

One important distinction between inductive and deductive reasoning is that solving problems deductively does not require knowledge obtained in the real world (Goswami, 2011). This means that deductive reasoning is finding solutions based on theoretical knowledge as opposed to finding solutions based on real life knowledge gathered. For example, the literature review of this study was done deductively to gather theoretical knowledge which assisted with the formulation of the themes that guided the inductive reasoning approach adopted for the study. The approach best suited to this research was inductive because the research started with observations; findings then were constructed using observations as the basis.



**Figure 3.3 Inductive research**

Figure 3.3 displays how inductive reasoning was applied to this study.

This study made use of deductive reasoning by gathering data deductively from literature sources to guide the interview and questionnaire questions. The results from the interviews and the surveys were then inductively analysed and presented.

### 3.1.3 Strategies

The strategy chosen for this study was a case study. Yin (1994) defines a case study as a way of conducting social science research. Furthermore, to answer research questions that contain the words 'how' or 'why', the preferred strategy is case study.

Yin (1994) mentions three categories of case studies These are:

- Explanatory
- Descriptive
- Exploratory



This exploratory case study focuses on collecting rich and thick data in a contemporary particularly bounded context (Yin, 1994). The impact of POPIA within SMEs will be subjective. Therefore, an exploratory case was selected. Methods used to gather information in this study included questionnaires and interviews. The information required for this study emanates from within the organisation that forms part of the study. Information-orientation sampling was used for the selection of the case (Flyvbjerg, 2006). The researcher has in-depth local knowledge of the case and it will therefore allow the researcher to “soak and poke” (Fenno, 1986).

### 3.1.4 Choices

In this section the methodological choices are discussed. These choices are:

- Quantitative methods
- Qualitative methods
- Mono-method
- Mixed method
- Multi-method

**Quantitative methods** characteristically involve the composing of survey questions, learning to count responses and to analyse data statistically (Nardi, 2015). This means that questions should be properly posed, the range of answers should be definite, and the data collected should be analysed numerically or mathematically. The theoretical work relating to the fundamental laws of mathematical sciences, like electromagnetic theory or the wave theory of light, are fully quantitative (Kuhn, 1962). This means that there is a relationship between mathematical sciences and quantitative studies.

**Qualitative methods**, on the other hand, ask open-ended questions which allow the respondents to answer in their own words, leading to a more complex response as opposed to a ‘yes’ or ‘no’ answer (Mack, Woodsong, Macqueen, Guest, & Namey, 2005). Furthermore, the analytical objective of the qualitative method is to describe the distinct responses, and these will be analysed textually as opposed to numerical or mathematical analysis.

**Table 3.2 Research methods comparison**

	Quantitative	Qualitative
<b>Analysis</b>	Mathematical (Kuhn, 1970), Numerical (Mack et al., 2005)	Grounded theory and inductive analytical strategies (Babbie & Mouton, 2000)
<b>Survey Questions</b>	Closed questions (Nardi, 2013)	Open-ended questions (Mack et al., 2005)
<b>Researcher Seeks</b>	Causal determination, generalization of findings and prediction (Hoepfl, 1997)	Knowledge of and inference to similar circumstances (Hoepfl, 1997)

The adoption of interpretivism as a philosophy by researchers was driven by the requirement to gather rich insights into an incipient phenomenon (Sahay, 2016). Weber (2004) argues that the difference between positivist and interpretivist researchers is evident in the research methods. One of the methods used by interpretivists to conduct their research is the case study (Weber, 2004).

**Mono-method** presents a threat to the validity of research by the bias of the mono-method when research conducted falls within a business setting (Donaldson & Grant-Vellone, 2002). The planned research will take place within a business setting. Therefore, mono-method research would not be feasible for this study.

**Mixed method.** Many authors argue that research is either an integration of, or there is an interrelation between, qualitative and quantitative research methods (Creswell, 1999). Referring to Section 3.1.4, the differences between the research methods are displayed, one of them being the differences in analysis. The data obtained for this study was analysed in a manner that integrated quantitative and qualitative research analysis methods. Therefore, the research choice for this study cannot be mixed method, as the research made use of qualitative methods only.

**Multi-method** is recommended by researchers to gain deeper, more meaningful and reliable perspectives on a specific topic (Cyr, Larios, Head, & Pan, 2009). Multi-method research was used in a step-by-step process using a systematic literature review and interviews as part of the design of a case study (Lytra, Sobernig, & Zdun, 2012). One way of characterising multi-

method research is differences in techniques focused on the formal qualitative custom (Collier & Elman, 2008). This study used interviews and surveys, both with open-ended questions.

### **3.1.5 Time horizons**

Cross-sectional and longitudinal refer to the research conducted and the time periods associated with it (Cherry, 2019). Longitudinal can be defined as collecting data from the same source over an extended period. Cross-sectional, on the other hand, is collecting data from a specific source at a specific point in time. This study was cross-sectional as data was collected at a specific point in time, from a specific group of people.

### **3.1.6 Techniques and procedures**

This section covers aspects relating to the data-collection methods employed by this study. Data-collection instruments and sampling techniques will be covered.

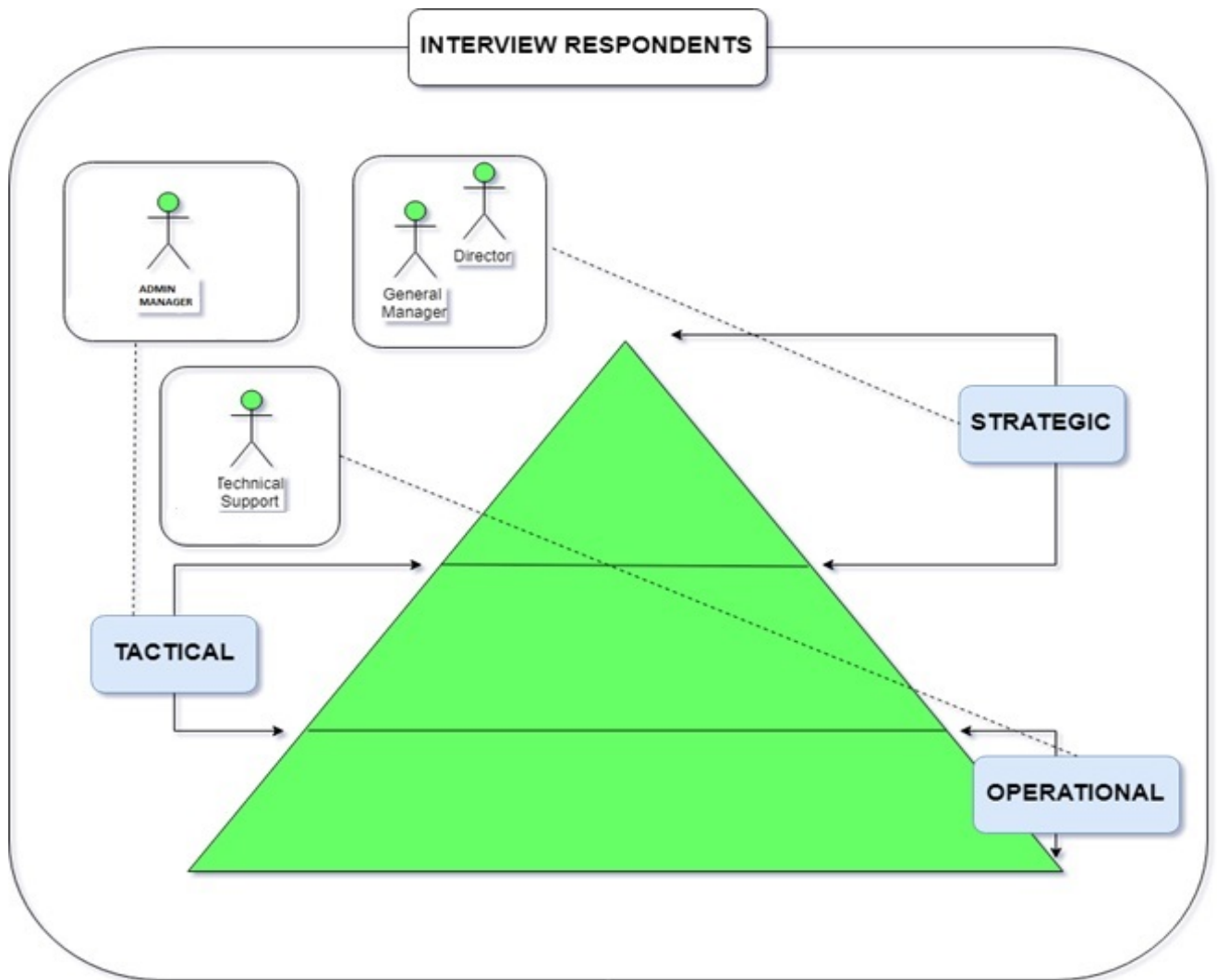
#### **3.1.6.1 Data collection**

Qualitative data-collection methods were used for gathering data. These entailed the use of semi-structured interviews and surveys containing open-ended questions. Interviews, which provide in-depth information, are often coupled with additional or supplementary forms of data collection which provide the researcher with a multi-faceted accumulation of information for analyses (Turner, 2010). Therefore, the qualitative data-collection methods used for this study were interviews and surveys.

#### **3.1.6.2 Interviews**

Interviews, when used as method of qualitative data collection, are quite common (Donalek, 2005). A semi-structured interview was used to allow for the possible emergence of new ideas gathered from the responses of the interviewees. Interviewees were asked if they were comfortable with the recording of the interviews, it was explained that they could request that the interview be stopped at any time, and they were assured of anonymity.

In order to group respondents and their individual responses, they were divided into three distinct organisational levels based on the Anthony Triangle (Anthony, 1965). This was done for triangulation. These hierarchical levels are depicted overleaf in Figure 3.3.



**Figure 3.4 Interview respondents**

The interviews were conducted with respondents from the strategic, tactical and operational levels. The same interview questions were asked to obtain a holistic view.

The interview respondents selected for a representation of the strategic level were:

- General manager
- Director

The interview respondent selected for representation of the tactical level was the Administration Manager.

The interview respondent selected for representation of the operational level was the IT Support Technician.

See Appendix B for Interview Protocol.

The interview consisted of five questions linked directly to the themes as presented in Chapter 2. The table overleaf represents the link between themes and interview questions.

**Table 3.3 Interview questions linking themes**

Theme	Question
<b>Consent</b>	Direct Marketing was impacted the most by POPIA because of its stringent consent requirement which states that written consent is needed, and I would like to know if you were aware of this and if it would have any impact on the business or its operations?
<b>Data officers</b>	The designation of an information officer is a requirement of POPIA, and its aim is to assist the business with matters relating to POPIA and I would like to know what your thoughts are about this?
<b>Deletion of personal information</b>	The request for deletion of personal information is a right granted to individuals by POPIA and I would like to know how the business will handle such a request and what are possible issues relating to this that you can foresee?
<b>Policies</b>	POPIA has a requirement that policies should be put in place to protect personal information and I would like to know what your thoughts are on that and if you have implemented or considered the implementation of such policies?
<b>Technical measures</b>	POPIA requires reasonable technical measures be put in place that secure personal information and if you could inform me of some of these measures and possibly their effectiveness?

Open-ended questions were asked which allowed the respondent to elaborate on his or her responses.

### **3.1.6.3 Questionnaire**

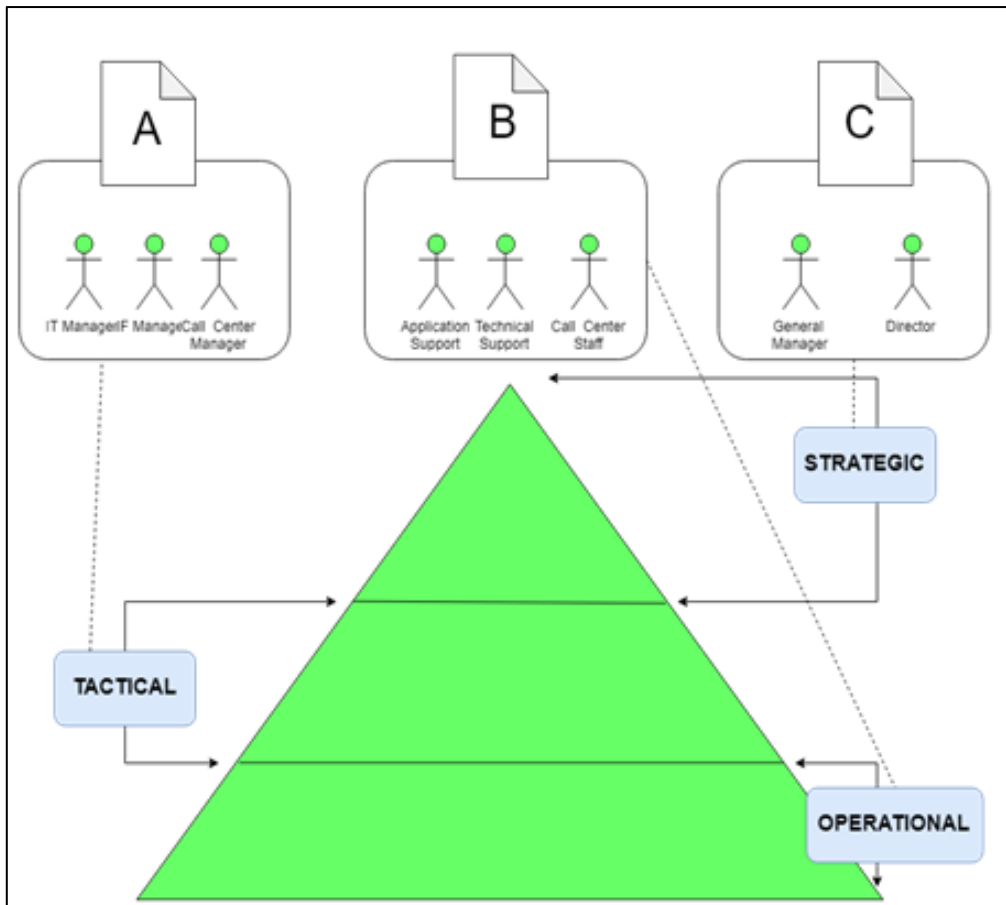
The survey was conducted using a questionnaire to answer the research questions. The questionnaires were paper based and presented to respondents to complete. As a security measure, internet access was limited for most users so online questionnaires were not considered. The surveys were conducted with respondents from all organisational levels. The

questionnaires had Likert-scale options that allowed the respondents to indicate how strongly they agreed with a specific statement.

**Table 3.4 Likert-scale value and meaning**

<b>Value</b>	<b>Meaning</b>
<b>1</b>	Disagree
<b>2</b>	Slightly
<b>3</b>	Partially
<b>4</b>	Totally agree

In addition to the Likert scale, respondents were given additional space to elaborate on their responses. Questionnaires were created with questions aimed at respondents at their specific organisational level. The figure overleaf shows how the questionnaires linked to the organisational level. Please note the question asked in the survey is, “How strongly do you agree with the statement?” The statements then contain the Likert-scale options.



**Figure 3.5 Survey respondents**

In the figure above, a letter is attached to a grouping of respondents which is then linked to the organisational level. The organisational levels are positioned at their respective hierarchical levels within a pyramidal structure. For example, Questionnaire A was linked to the respondents that are managers; these managers were then linked to the tactical organisational level. Secondly, Questionnaire B was linked to the respondents that are support and call centre staff, which were then linked to the operational organisational level. Lastly, Questionnaire C was linked to the director and general manager, which were linked to the strategic organisational level.

Questionnaire C (Appendix C) was handed to strategic-level role players because it contained questions more relevant to them. Strategic-level personnel and respondents selected were:

- General manager
- Director



The six survey statements were linked directly to the literature themes. The table below matches the statements with the themes.

**Table 3.5 Questionnaire C themes and statements**

Theme	Statement
Policies (2.4)	<ul style="list-style-type: none"> <li>▪ Policies are put in place that ensure data integrity and confidentiality when communicating with clients via email.</li> <li>▪ Information security policies are in place to protect client information in general.</li> </ul>
Technical measures (2.5)	<ul style="list-style-type: none"> <li>▪ The company has implemented reasonable technical measures that deal specifically with the protection of personal information.</li> </ul>
Consent (2.1)	<ul style="list-style-type: none"> <li>▪ The company always gets consent from clients to use and store their personal information.</li> </ul>
Data officers (2.2)	<ul style="list-style-type: none"> <li>▪ The company has started planning for the designation of an Information Officer as required by POPIA.</li> </ul>
Deletion of personal information (2.3)	<ul style="list-style-type: none"> <li>▪ The company will be able to handle a request for deletion swiftly and accurately.</li> </ul>

Questionnaire A (Appendix D) contained statements that were more relevant to the tactical level personnel and respondents selected were:

- Administration manager
- Finance manager

- Call centre manager

The ten survey statements were linked to the literature themes, but this specific questionnaire was more focused on topics relating to the theme, technical measures. Risky behaviour by users was identified by literature as one of the biggest threats that could compromise technical measures put in place to secure infrastructure and information.

The table below matches the statements with the themes:

**Table 3.6 Questionnaire A themes and statements**

Theme	Statement
<p><b>Policies (2.4)</b></p>	<ul style="list-style-type: none"> <li>▪ You are aware of policies within your organisation that provide guidelines for ensuring that emails sent to clients are protected.</li> <li>▪ You always confirm that it is the correct client email that you have on the system.</li> </ul>
<p><b>Technical measures (2.5)</b></p>	<ul style="list-style-type: none"> <li>▪ You allow other users to make use of your computer while logged in with your details.</li> <li>▪ You use the same password for logging on to your workstation as you use for logging on to social networking sites.</li> <li>▪ One or more of your colleagues knows your password to sign into your windows PC.</li> <li>▪ You make use of the USB port on your workstation computer to charge your cell phone.</li> <li>▪ You always lock your PC when you leave your desk.</li> <li>▪ You make use of USB devices on your workstation to share media (music, images, etc.)</li> <li>▪ You are familiar with the term 'phishing'.</li> <li>▪ Your Windows operating system is up to date.</li> </ul>

Questionnaire B (Appendix E) contained statements that were more relevant to the operational level. These role players are listed below:

- IT Technical support technician
- Application support technician
- Call centre staff

The three survey statements were linked to three of the five literature themes. The table below shows the link between the theme and the statement.

**Table 3.7 Questionnaire B themes and statements**

Theme	Statement
Policies (2.4)	<ul style="list-style-type: none"> <li>• Policies are put in place that ensure data integrity and confidentiality when communicating with clients via email.</li> </ul>
Technical measures (2.5)	<ul style="list-style-type: none"> <li>• Information security control mechanisms are in place to protect client information.</li> </ul>
Deletion of personal information (2.3)	<ul style="list-style-type: none"> <li>• The company will be able to handle a request for deletion swiftly and accurately.</li> </ul>

The table shows the theme referring to the literature review chapter.

#### **3.1.6.4 Data analysis**

Interview data collected was analysed qualitatively and survey data was analysed qualitatively, enabling descriptive statistics. The tool utilised for analysis was ATLAS.ti. It is stated that using qualitative software might lead to an increase of rigour in research (Lu & Shulman, 2008). Responses were analysed using coding. Coding is when text is used as data; this data is then broken up or grouped into something meaningful such as codes (St. Pierre &

Jackson, 2014). Furthermore, codes can be ordered thematically which will allow for emergence of additional themes. Coding is considered one of the most important analytical steps that assists with the organisation of textual data (Basit, 2003). ATLAS.ti allows for the grouping and ordering of codes. Analysis of empirical data led to the emergence of a codebook (Appendix L).

## **3.2 Research methodology**

Research methodology can be interpreted as the science of how research is conducted in a scientific manner (Kothari, 2004). In the previous section, the research methods were identified where focus was placed on the methods and techniques intended to be applied to the study. This section will discuss how these methods and techniques were applied.

### **3.2.1 Sampling**

The population comprises SMEs within the Western Cape in the medical insurance industry that develops in-house software. Non-probability sampling of convenience was used as a sampling technique. The technique was selected because the respondents were easily accessible to the researcher. The following sub-sections will give a brief description of the application of the techniques. Furthermore, target population availability in terms of time availability was an additional contributing factor for selection.

For this study, an SME in Cape Town, Western Cape, in the medical insurance industry that deals with sensitive medical information of its clients was identified as the research case. It deals with personal information of both its clients and personnel. It has an in-house software development team that develops and maintains its own software and database.

The director and the general manager of the company were chosen as participants because of their familiarity with the processes within the company. The IT application support assistant, a respondent representing the operational organisational level, was selected as a participant as he deals with various tasks which include uploading of policy documents and the generating and testing of schedules to confirm that the correct information is displayed. Security questions will be best answered by the IT support technician, another respondent representing the operational organisational level, as he is responsible for the security of the network and user accounts, and manages backups that run off site to a secure remote location. Operational level staff were chosen as participants as well as they deal with clients daily and frequently

deal with sensitive information, and the questionnaires were used to gather descriptive statistics. Most of the questionnaire respondents were from the operational organisational level and had more actors. Only one representative of the different organisational levels was chosen to participate in the interviews.

Table 3.8 depicts the levels and roles of the units, the techniques, and the sub-question that relates to this technique.

**Table 3.8 Levels, roles, techniques and research questions**

Levels	Roles	Techniques	Research Questions
<b>Strategic</b>	General Manager	Interview	MQ What implementation guidelines should be considered by SMEs to promote compliance with POPIA?  SQ1 What are current challenges that SMEs could face when implementing POPIA compliance?  SQ2 How can POPIA compliance implementation challenges be met?
	Director	Survey	
<b>Tactical</b>	Administration Manager	Interview	
	Finance Manager	Survey	
	Call Centre Manager		
<b>Operational</b>	IT Technical Support	Interview	
	IT Application Support	Survey	
	Call Centre staff		

### 3.2.2 Data-collection methods

All respondents, both interview and survey, were introduced to the study. The aim and purpose of the data collection were explained to them. They were informed that participation was completely voluntary and that they would not be prejudiced in any way should they choose to not participate. The study was conducted in the work environment during working hours from 08:00 to 16:00.

Interviews were scheduled with respondents via email. Respondents were interviewed during their normal hours of work and were conducted on a one-on-one basis. Interviews were recorded using a Samsung Galaxy S7. The interview recordings were uploaded and stored using Microsoft OneDrive. The storage facility allowed for a file structure type of saving. Transcription involved retrieving of the audio files, playing them back, then typing the responses in a Microsoft Word document (Appendix H, Appendix I, Appendix J). These files were then converted to PDF format and uploaded into ATLAS.ti. The table below lists the respondents and their organisational level, and the transcription added as appendix:

**Table 3.9 Interview respondents with role and appendix**

Organisational level	Role	Appendix
Strategic	GM	Appendix H
Tactical	AM	Appendix I
Operational	ITST	Appendix J

The interviews were conducted in order of organisational level as listed above.

The surveys were conducted by paper. The reason for this was that internet access was limited, as a safety precaution, for all respondents participating in the survey. These surveys were named according to colour group, organisational level, and the number of the survey. For example, Survey 1, from the red group and in the operational level, was named RQC1. The respondents that received the surveys had to be grouped. This was done to allow departments to function while respondents were taking the survey. In addition to this, the space offered to conduct the survey could not hold all the respondents at once. The groups were named according to colours. In addition, these colour groups formed part of the naming convention for the individual surveys.

The table below illustrates the grouping:

**Table 3.10 Survey colour coding and prefix**

Colour Code	Prefix	Number of respondents	Organizational Level
Blue	BQ	6	Operational
Green	GQ	6	Operational, Tactical
Purple	PQ	5	Operational, Tactical
Red	RQ	4	Operational, Tactical
Yellow	YQ	1	Strategic

As indicated in the table above, surveys from the colour group blue would have the letter 'B' that would indicate that the specific survey was part of the blue group, while the letter 'Q' signified questionnaire. Furthermore, if this specific questionnaire was given to a role player from the operational level and it was the third questionnaire, it would be named BQC5. All the surveys were scanned to PDF format. These were stored using Microsoft OneDrive. These results were then retrieved and captured into Microsoft Excel spreadsheets and subsequently imported into ATLAS.ti. The naming of the columns in the Excel documents had to be done in a specific manner to ensure that the data was imported correctly into ATLAS.ti.

Most of the questionnaire questions were open-ended but also contained close ended questions.

### **3.2.3 Case description**

The organisation was based in the Cape Town CBD, Western Cape. The organisation develops and maintains the main business application.



### 3.2.4 Unit of analysis

The study used the organisation as the unit of analysis. The table below shows the unit, organisational levels, and roles

**Table 3.11 Unit of analysis, organisational level and roles**

Unit of analysis	Organizational Level	Role
The organisation	Strategic	General Manager
		Director
	Tactical	Administration Manager
		Call Centre Manager
		Finance Manager
	Operational Level	Call Centre Staff
		IT Application Support
		IT Technical Support

Table 3.11 concludes this section.

### 3.2.5 Ethical considerations

Ethical considerations should be applied to prevent the abuse of the participants (Ponterotto, 2010). In the United States of America, federal laws have promulgated regulations to protect the rights of human participants taking part in research (Brogt, Dokter, Antonellis, & Buxner, 2009). One of the ethical challenges relevant to qualitative issues relates to informed consent procedures (Houghton, Casey, Shaw, & Murphy, 2010).

Ethical clearance was obtained and is included as Appendix A. Ethical clearance was also obtained from the company at which the research was conducted. Consent in principle for the collection of data had been obtained from the SME which allowed the researcher to conduct his research at the company. Appendix F is the introductory letter for collection of research data that was presented to the General Manager. Appendix G is the signed consent in principle form whereby consent was granted to the researcher to collect data from the organisation. The participants were informed regarding the nature and purpose of the study. They were assured that data was collected for research purposes only and that the data collected would not be used against them in any way. In Appendices B, C, D and E it was stated that signing the questionnaire or interview form by the respondents indicated that they were informed about

the nature of the study, they were guaranteed anonymity, they had the right to refuse to participate at any point, and that their confidentiality was guaranteed. These ethical considerations were read to the respondents prior to the dissemination of the questionnaires, and an opportunity was given to them to ask questions for clarification if they were uncertain of anything. The same considerations were applied to the interviewees.

### **3.2.6 Trustworthiness**

In qualitative terms, validity refers to the accuracy whereby the findings precisely and accurately reflect the data (Noble & Smith, 2015). Furthermore, reliability refers to the uniformity of the analytical procedures, including the clarification of any research method or personal bias that could have affected the findings. The criteria for trustworthiness are described as parallel to rigour (Lincoln & Guba, 1985). Furthermore, there are four criteria identified as contributors to the trustworthiness of a study:

- Credibility
- Transferability
- Dependability
- Confirmability

Techniques play an important role in meeting the criteria, either in a positive or negative way.

The table below represents the criteria and techniques that contribute towards achieving trustworthiness.

**Table 3.12 Lincoln & Guba’s (1985) trustworthiness criteria & techniques for establishing them**

Criteria	Techniques
Credibility (internal validity)	1) Prolonged engagement (pp. 301-304) 2) Persistent observation (pp. 304-305) 3) Triangulation (sources, methods, investigators) (pp. 305-307) 4) Peer debriefing (pp. 308-309) 5) Negative case analysis (pp. 309-313) 6) Referential adequacy (pp. 313-314) 7) Member checks (pp. 314-316)
Transferability (external validity)	8) Thick description (p. 316)
Dependability (reliability)	9) Overlap methods (Triangulation of methods) (p. 317) 10) Dependability audit – examines the product to attest that the findings, interpretations & recommendations are supported by data (pp. 317-318)
Confirmability (objectivity)	11) Confirmability audit – examines the product to attest that the findings, interpretations & recommendations are supported by data (pp. 318-327)
All four criteria	12) Reflexive journal (about self & method) (p. 327)

The next subsections will examine techniques applied to increase the probability of meeting the criteria.

**Credibility** can be achieved through triangulation. Triangulation is a technique that can contribute to the credibility of a study (Lincoln & Guba, 1985). Triangulation refers to a process that requires three measurements within a specific landscape to uncover the commonality (Meijer, Verloop, & Beijaard, 2002). Triangulation requires three measurements in the same landscape to be effective. Triangulation is the term used in social research that refers to the observation, with a minimum of at least two points or perspectives, of the research (Flick,

2004). This means that triangulation can be only performed where there are multiple perspectives. Furthermore, triangulation can be done from a methodological perspective, between methods like scale- valued questionnaires or interviews. Likert-scale questionnaires and interviews were used as part of the study. Triangulation of measurement processes can yield powerful evidence (Elman, 1995). Triangulation can be done between methods which could comprise surveys or semi-structured interviews (Farquhar & Michels, 2016). In this study, the respondents were divided into three organisational levels. In addition, semi-structured interviews as well as surveys were used to collect data.

**Transferability** in this study refers to how well the data, thick and rich, is presented and how others can apply it in similar contexts (Lincoln & Guba, 1985). The aim of this research is to provide a set of guidelines that can be utilised by other SMEs as an aid to POPIA compliance.

**Dependability** refers to a judgement made by a capable and disinterested external auditor that determines whether an audit trail exists (Lincoln & Guba, 1985). This means that an individual acting as an auditor, who has no knowledge of the research or the topic for that matter, must be able to conclude that procedures were followed in an objective manner.

**Conformability**, which is part of the aforementioned audit, is focused more on the data and its reconstructions (Lincoln & Guba, 1985). This means that an external auditor must, objectively, be satisfied with the data and the reconstruction of it.

In closing, this study made use of triangulation methods to enhance its credibility. The topic of the study, which is centred on POPIA, does improve the transferability, as the findings could assist other SMEs. The research design maps the scientific procedures involved with the collection and analysis of data, thus providing an external auditor or reviewer with the relevant information required to determine dependability and conformability.

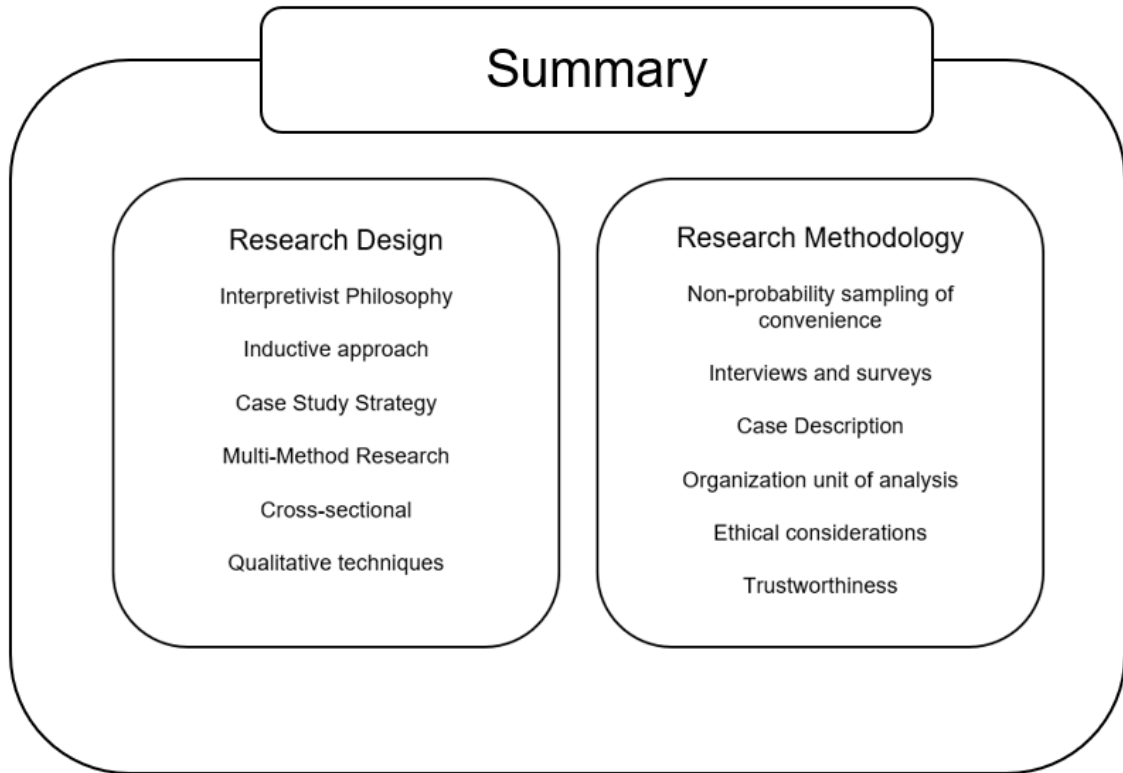
### **3.2.7 Delimitation**

This study explored the steps to be taken within an organisation that can promote compliance with POPIA, specifically regarding the themes extracted by the literature review. It included only respondents from Manage Plus that are responsible for implementation of POPIA requirements. It did not include any form of implementation.

This study excluded requirements not identified as themes during the pre-literature review.

### 3.3 Summary

The research design section outlined the plan to follow when answering the research question. Figure 3.6 summarises the design and methodological choices of the study.



**Figure 3.6 - Research design and methodology summary**

The research methodology section conveyed how the planned design was carried out. The philosophy adopted for the study is interpretivist and qualitative methods were utilised to meet the objectives of the study. The population for sampling and units were identified, the interview and survey were drafted, ethical clearance was obtained, and the analysis technique was identified. In the next chapter, the findings are presented.

## 4 CHAPTER FOUR: FINDINGS AND ANALYSIS

*“Do your little bit of good where you are; it's those little bits of good put together that overwhelm the world” – Archbishop Desmond Tutu*

In Chapter 3 the research design and methodology for the study were presented. Chapter 4 focuses on the findings and the analysis of the collected data. For the sake of authenticity, the grammatical structure of the quotations has not been changed.

As a recapitulation, the data collected for this study was obtained using semi-structured interviews and surveys. Interviews and surveys were conducted with employees from the strategic, tactical and operational levels within the organisation situated in Cape Town, Western Cape. Roles of the participants were:

- General manager (strategic)
- Administration manager (tactical)
- Call centre manager (tactical)
- Intermediary finance manager (tactical)
- IT support technician (operational)
- Call centre agent (operational)

Throughout this chapter, the respondents are referred to as follows:

- General manager [GM]
- Administration manager [AM]
- Call centre manager [CCM]
- Intermediary finance manager [IFM]
- IT support technician [ITST]
- Call centre agent [CCA]

The roles, organisational levels and references are displayed in Table 4.1 below.

**Table 4.1 Roles, organisational levels and references**

<b>Role</b>	<b>Organisation Level</b>	<b>Reference</b>
General Manager	Strategic	GM
Administration Manager	Tactical	AM
Call Centre Manager	Tactical	CCM
Intermediary Finance Manager	Tactical	IFM
IT Support Technician	Operational	ITST
Call Centre Agent	Operational	CCA

Table 4.1 above represents the grouping of roles at the organisational level, including the references in this chapter. The data derived aims to answer secondary research questions SQ1 and SQ2 (Section 1.3, Research Objective and Questions). Graphs are included as a representation of responses.

The reporting is thematic. In addition, reporting is done according to the organisational levels of respondents. The sections are presented as indicated below.

**Table 4.2 Theme and section**

<b>Theme</b>	<b>Section</b>
<b>Consent</b>	<b>4.1</b>
<b>Cross-legislation impact*</b>	<b>4.2</b>
<b>Data officers</b>	<b>4.3</b>
<b>Deletion of personal information</b>	<b>4.4</b>
<b>Industrial regulatory requirements*</b>	<b>4.5</b>
<b>Information management*</b>	<b>4.6</b>
<b>Information privacy*</b>	<b>4.7</b>
<b>Policies</b>	<b>4.8</b>
<b>Reasons for compliance battle*</b>	<b>4.9</b>
<b>Technical measures</b>	<b>4.10</b>

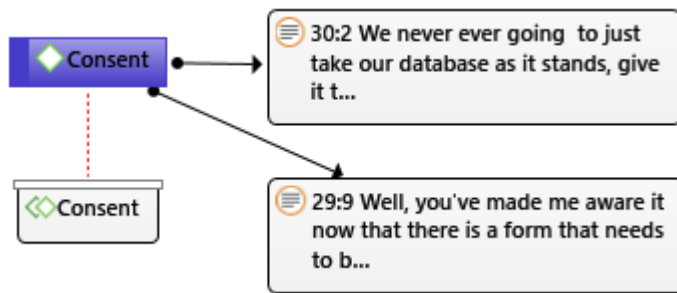
The themes marked with an asterisk (\*) indicate that the theme emerged from analysis.

#### **4.1 Consent**

This section reviews the empirical data relating to the theme 'consent'. Consent was identified as one of the main requirements of POPIA.

When questioned regarding consent during the interview with the AM, she stated that she was not even aware that a signed form is required for consent. The GM stated that no marketing is done at the organisation.





**Figure 4.1 Consent**

In Figure 4.1, the codes and quotations are linked to the theme. The quotation 30:2 links to the code consent which is based on responses that speak to issues of consent.

The literature pointed out the importance of obtaining consent from individuals. The tactical perspective indicated that there was no awareness of a requirement of POPIA to gain consent in writing for direct marketing. The strategic perspective pointed out that direct marketing was of no impact to the business.

## **4.2 Cross-legislation impact**

In this section the data-derived theme, cross-legislation impact, is discussed. The theme is divided into two categories:

- FAIS Act (4.6.1)
- FICA Act (4.6.2)

These categories emerged from the empirical data and link to the theme 'cross-legislation impact'. This section reports on the empirical findings relating to these categories.

### **4.2.1 FAIS Act**

Information is retained to assist with queries that are handed over to the ombudsman [ITST]. The ITST stated:

The reason why we need to keep that is if they go to the ombudsman or there's something related when they had the policies, we need to be able to go back and give them info on that specific query that have.

The timeframe to store personal information as specified by FAIS is contradictory with POPIA and the company still operates in compliance with FAIS, which is to store information for at least five years [GM]. The GM commented:

... you need to delete people's information after x amount of time, etc., and at the time it was contradictory to what the FAIS act stipulates.

Hard copies are discarded, and soft copies retained as these are acceptable by FAIS [GM]. The GM commented:

... we destroy the hard copy once we've confirmed we have a soft copy because the FAIS Act states that we only need to have a soft copy, we don't need both ...

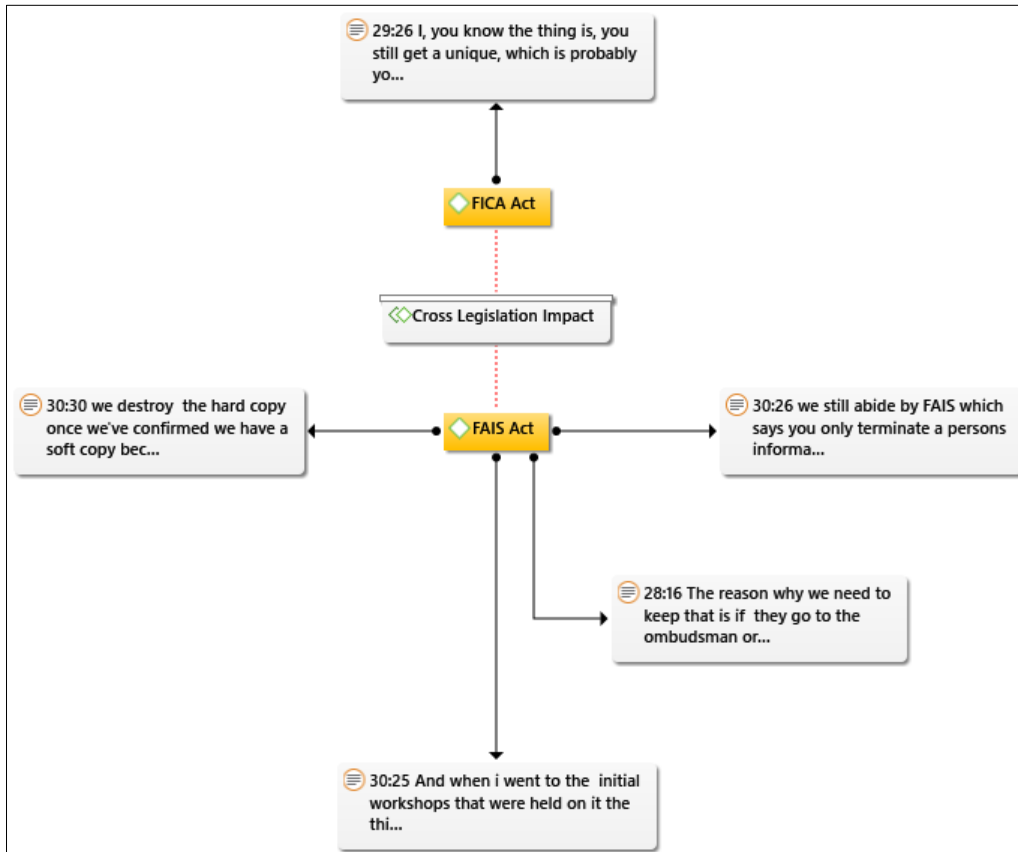
#### **4.2.2 FICA Act**

A third-party information provider is used to check whether ID numbers are valid as part of the FICA requirements. This allows for viewing additional information about the ID number holder and could put individuals at risk of having their personal information compromised [AM]. The AM commented:

I, you know the thing is, you still get a unique, which is probably your ID number, which I can still put in ITC, I can put in a number on any other platforms and still find out who you are, I'm not interested in who you are, I know this sounds terrible, coming from "We must know our clients", you know, FICA, know your client ...

In summary, the operational perspective showed information is retained to assist in the event of its being needed by the ombudsman. The strategic perspective pointed out that a FAIS requirement to store such information for five years currently exists. POPIA, however grants individuals the right to have their information deleted. Additionally, from the strategic point of view, FAIS accepts soft copies of information and therefore hard copies are destroyed. The tactical viewpoint indicated that ID numbers do get shared with a third party to gain personal information relating that specific ID number. Furthermore, accessing ITC does however provide personal information to the viewer which could be used to the detriment or advantage of an individual. The operational and strategic perspectives were aligned by the mutual awareness of legal implications regarding storing data. The strategic perspective indicated that POPIA contradicts the FICA Act. The tactical perspective showed that it is a legal requirement to retrieve personal information from providers like ITC. Furthermore, such information could

be used to the detriment of an individual. General awareness regarding the different legislation across the organisational levels shows a mutual understanding of legislative adherence as well as the reasons for it. The impact POPIA has on these additional legal requirements has been established. In the figure below, we can see the category cross-legislation impact with the codes FAIS Act and FICA Act.



**Figure 4.2 Cross-Legislation impact**

In Figure 4.2 the relationships between the theme, the codes and the quotations are displayed by means of a red dashed line. Furthermore, the relationships between codes and responses are displayed by means of a black arrow. From the diagram we can see how the text relates to the theme, for example, quotation snippet 30:26 speaks about FAIS. Therefore, the quotation was linked to this theme.

### 4.3 Data officers

This section reviews the empirical findings associated with the theme 'data officers' (2.2). It closes with a summary of the findings.

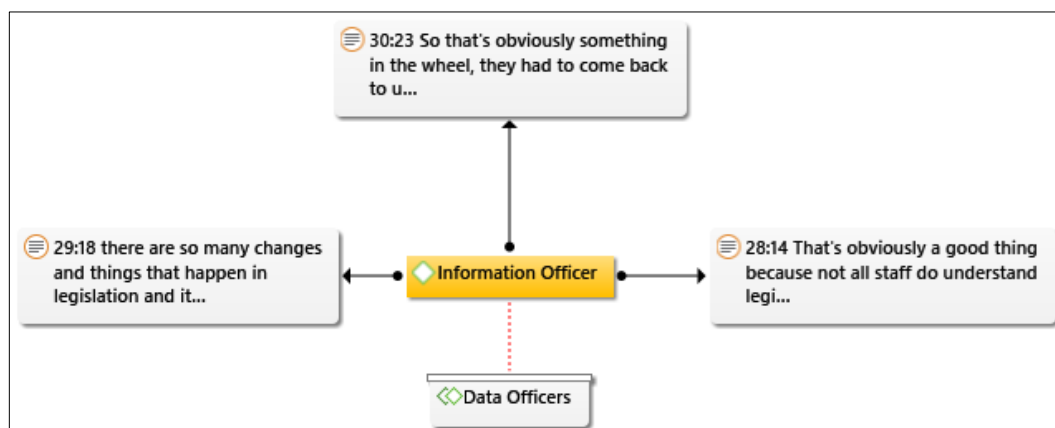
It is beneficial to have an information officer as this individual will be able to translate POPIA requirements to staff [ITST]. It would be beneficial to have an individual that keeps staff up to date with the latest changes to legislation as this occurs quite frequently [AM]. The AM commented:

... there are so many changes and things that happen in legislation and it's just changing all the time, it's a living dream thing, that it is good to have an appointed person that is up to date with whatever changes are happening to actually feed that through because you work for the industry ...

The process of designating an information officer will be started as soon as the Act comes into full effect [GM]. The GM commented:

So that's obviously something in the wheel, they had to come back to us and say, "Now you need to have an official appointed information officer like you do a compliance officer and this is the process." We would follow the process.

In closing, the benefits of having an information officer is evident in the statements made by the IT support technician and the administration manager. The only hurdle the company currently faces is that the Act is not yet in full effect, as stated by the general manager. The figure below is a network diagram of the theme in relation to the codes and the responses.



**Figure 4.3 Data officer**

In the figure above, the relationships between the theme and the codes are displayed by means of a red dashed line. From the diagram we can see how the text relates to the theme, for example, text snippet 30:23 speaks to the information officer. Therefore, the text was linked to this theme.

In closing, literature stressed the benefits of having an information officer. In addition, findings indicated that across organisational levels there is mutual agreement that an information officer is an important and beneficial individual in an organisation.

#### **4.4 Deletion of personal information**

This section reviews the empirical findings associated with the theme 'deletion of personal information' (2.3). POPIA grants individuals the right to request deletion of their information. This is a common right across the diverse data protection legislation that constitutes part of this study.

Backups of data are required, and data needs to be stored for five years. Backups happen frequently, and deletion of information is possible although time consuming [ITST]. The ITST commented:

... that information needs to be kept for another five years OK, and after five years we can say OK, cool, let's clean off the data that we don't need ...

In terms of fraud and fraud prevention, certain types of information should not be allowed to be deleted as this information is used to protect the business [AM]. Personal information retained should be held for ethical or business processes only and not for the exploitation thereof, and the holders of personal information should be responsible for its guarding and safekeeping [AM]. The AM commented:

For your own operational business not necessarily to exploit that person and, you know, maybe have that data go to another company, that company then contacts the client for another product and now you're getting a cutback from that company as well, a commission or something, you're servicing yourself, you're not, it's got to be for moral reasons that you need it, for ethical reasons for running your business.

When viewing personal information, it should be done for a specific and legal purpose and not for malintent [AM]. The AM commented:

... there should still be consequences to the holding of that information, so that information somehow leaves that company and lands in the wrong hands, you as the company, you're responsible for that information. So, if you decide, and there is a

law that says you don't have to delete, you need to be responsible for that dataset.

Information is retained to allow for analysis and identifying anomalies [AM]. She commented:

I've had a forensics background and you know, you, a lot of your indicators are from you analysing data, okay, whether that is people's personal information, if it's based on a geographical area or whatever the case may be, it's based on links and nodes and tying up information to try and determine a way forward if you're looking at fraud and that kind of thing and having an indicator of five clients that maybe came through during the year and there was fraud allegations etc, needing to know that information should they apply again at a later stage because now the insurer has the right to give them thirty days' notice without going into any much detail.

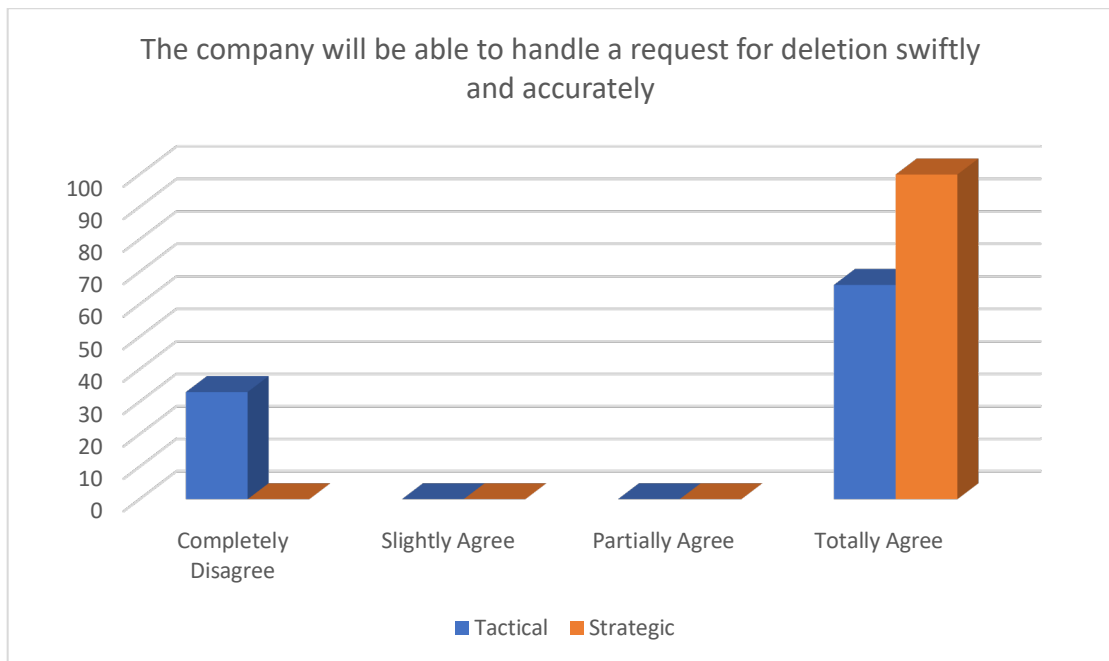
Information is shared among service providers to prevent fraudulent activities [AM]. The AM commented:

... forensics staff would come together once month and you would share information on the service providers, mostly doctors, hospitals, pathologists, that type of thing. You'd share the information in terms of the fraud, in terms of the billings, and they would go back, and they would go through the entire dataset ...

A process is in place that handles the deletion of emails, and information reviews are done monthly to determine which information is to be removed and deleted from the system [GM]. The deleting or masking of information would still render the data unreadable to a user [GM]. She commented:

So, in my mind, deleting or masking, it's probably the same thing. The average person in the office isn't going to go and be able to access that person's information after that set amount of time.

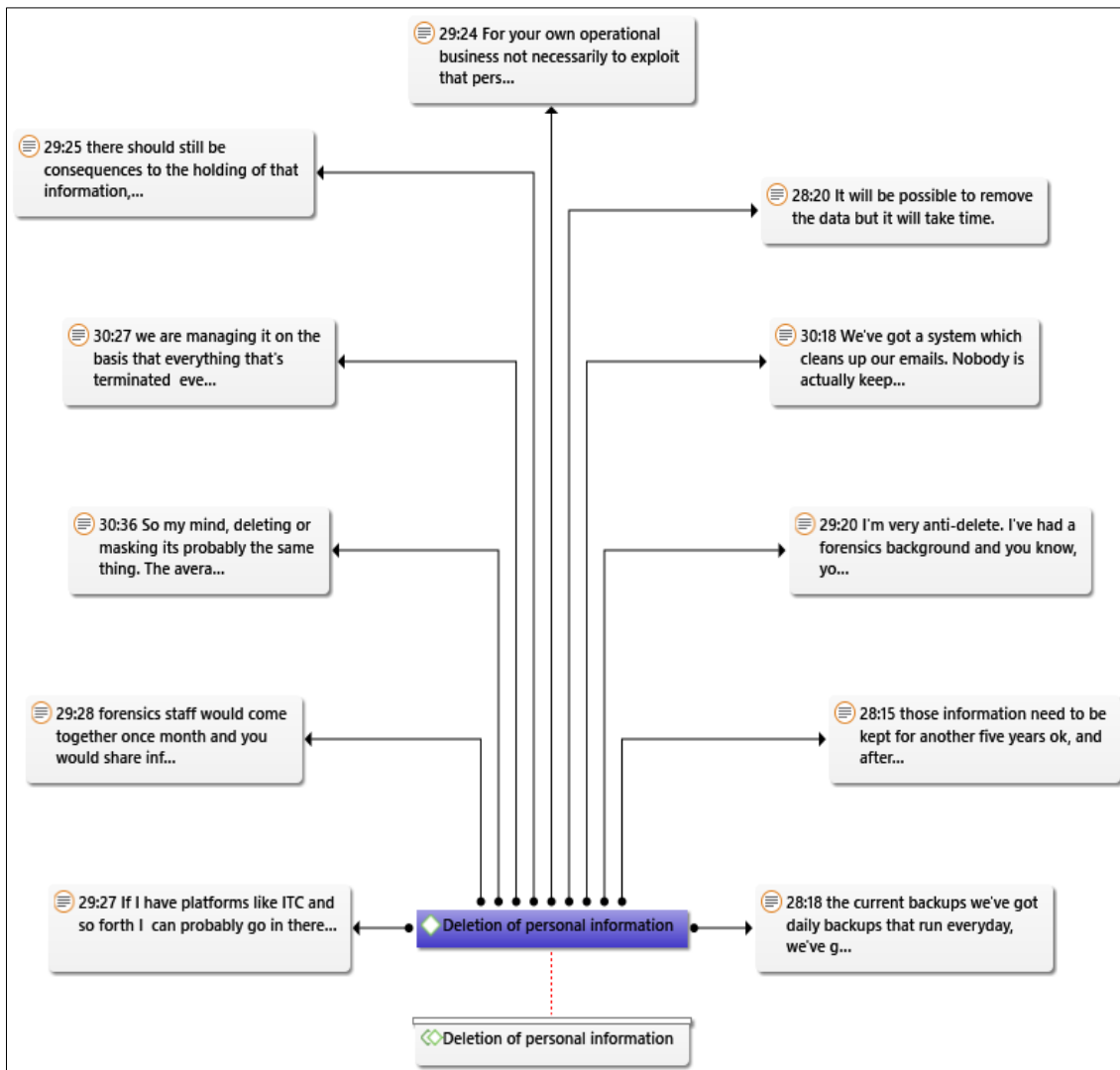
The graph overleaf depicts the responses from the tactical and strategic organisational levels to the statement: "The company will be able to handle a request for deletion swiftly and accurately." The statement can be found in Questionnaires A and B (Section 3.1.6.4) as Questions 6 and 3, respectively.



**Figure 4.4 The company will be able to handle a request for deletion swiftly and accurately**

The strategic level respondent(s) agreed fully with the statement. There was a difference between the responses of the tactical level, with two agreeing completely and one completely disagreeing, respectively. The data displays that there are conflicting views between strategic and tactical levels regarding the company’s ability to carry out a request for deletion.

In summary, it appears that the various organisational levels have different views regarding deletion of information. From an operational perspective, there is awareness of the five-year retention period for information and that deletion is possible albeit time consuming. The tactical perspective was that certain types of information should not be removed in order to combat fraud. Furthermore, this information is shared among service providers to assist in the fight against fraud. An additional tactical perspective was that when deletion is not possible, the information held should be done so responsibly. The strategic perspective was that monthly information reviews are done to determine the information to be deleted. Furthermore, a recommendation was made to consider masking of data, rendering the data unreadable by users that have access to this data, as opposed to deleting the information. The diagram overleaf illustrates the grouping of the theme, the code and the responses.



**Figure 4.5 Deletion of personal information**

In the figure above, the relationships between the theme and the codes are displayed by means of a red dashed line. From the diagram we can see how the text relates to the theme, for example, text snippet 30:36 speaks about deleting. Therefore, the text was linked to this theme.

#### **4.5 Industrial regulatory requirements**

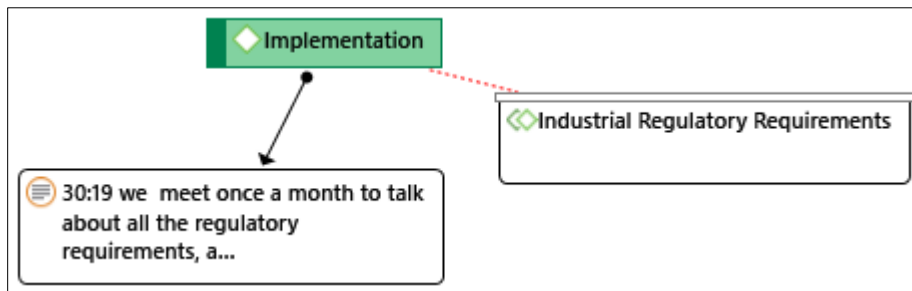
Industrial regulatory requirements comprise a further category that emerged from the empirical findings.



The General Manager commented:

... we meet once a month to talk about all the regulatory requirements, any changes in the industry, so if any new Act comes into play we would talk about it, we would meet on it, and then we would every month when we meet we would say right, three months ago we implemented the POPIA process into the company ...

The image below shows the network diagram of the theme 'industrial regulatory requirements'.



**Figure 4.6 Industrial regulatory requirements**

In the figure above, the relationships between the theme and the codes are displayed by means of a red dashed line. Furthermore, the relationships between codes and responses are displayed by means of a black arrow.

The strategic perspective indicated that monthly meetings are held to ensure that the organisation meets regulatory requirements. Furthermore, ongoing updates on previously implemented requirements are provided.

#### **4.6 Information management**

The theme 'information management' emerged from analysis as a new theme.

This section reports on the findings linked to the sub-categories which are:

- Validation (4.7.1)
- Verification (4.7.2)

#### **4.6.1 Validation**

A validation process is in place when communicating with clients as a means of ensuring that they are contacting the correct individual. In the event of disclosure of personal information to a third party, consent is requested from the individual [AM]. Alternative methods of validating an individual are considered [AM]. The AM commented:

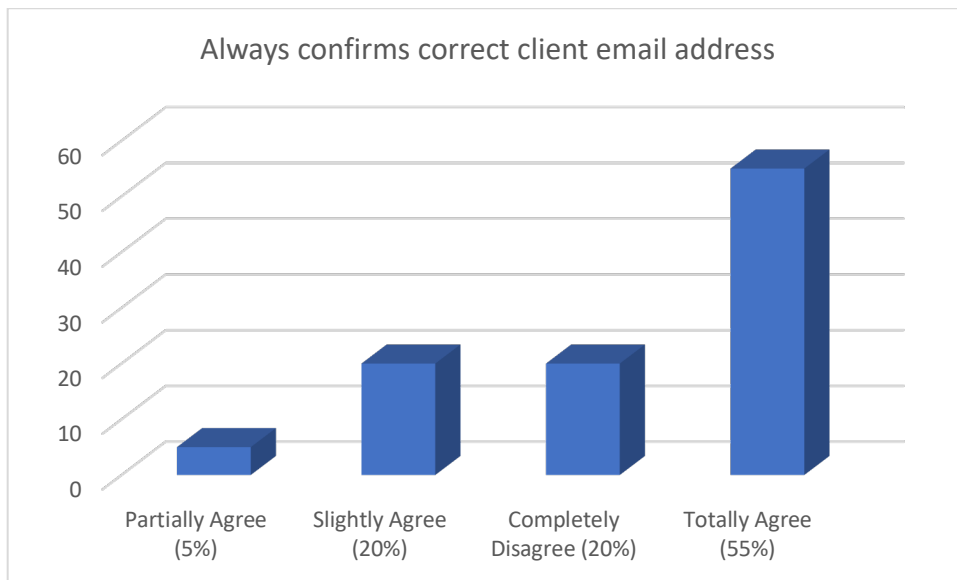
We don't disclose information, as a rule, to any party other than the principal insured of the policy and if there is a request by a spouse for some form of information we ask that we receive an email from the principal insured stating that they don't mind that the spouse, or the name of the spouse, ID etc., where they live.

#### **4.6.2 Verification**

Call verification is one of the most fundamental aspects of the policy process and all information is verified before it is captured on the system. This includes information like confirming ID numbers and names. All verification calls are recorded [GM]. The GM commented:

... we verify everything, right down to this is your name, we double check your ID number, your bank details, you did fill in the form, you did meet with that person, you know what the policy is about, you know what you are going to be paying, you know how often you are going to be paying, you know what cover you've got, what it includes, what it excludes, all those types of things.

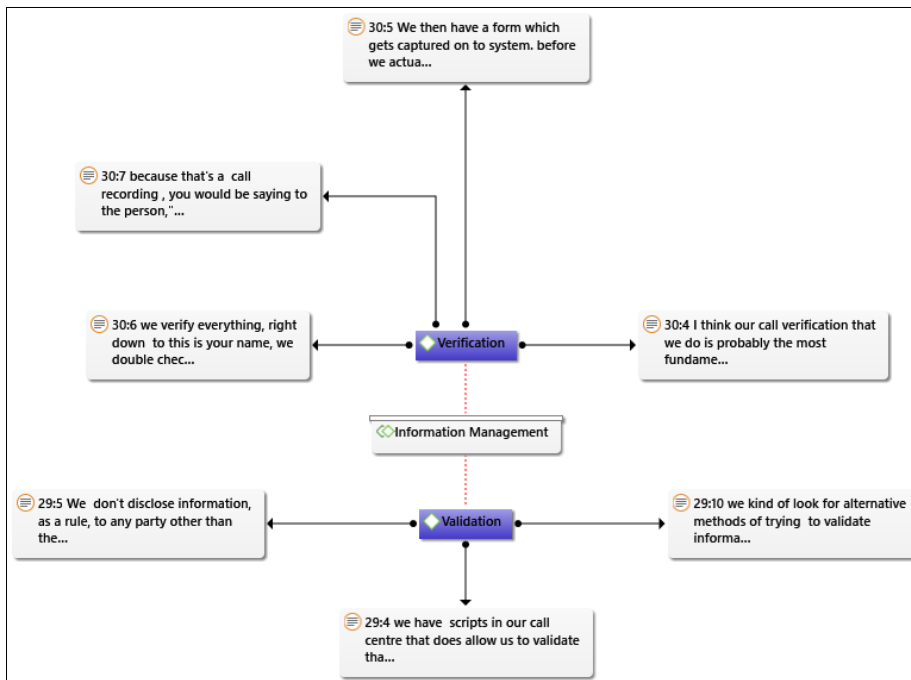
The figure overleaf displays the Likert scale results of the statement: "Always confirms correct client email address" which was listed in Questionnaire B, Question 3.



**Figure 4.7 Always confirms correct client email address**

Slightly more than half of the operational level respondents agreed fully with the statement. Slightly less than a quarter were in complete disagreement and slightly agreed. Very few agreed partially with the statement. From an operational perspective, it could be inferred that users depended on information stored in the business database and this information is correct. There were concerns regarding the timeliness of the information. A small representation showed disregard for procedures in their responses. The strategic perspective indicated that rigorous verification processes are in place to ensure the information captured is accurate. The tactical level indicated that an information validation process is in place to ensure that the correct individual receives the correct information. Across organisational levels, respondents were aware of procedures put in place to validate email addresses.

The network diagram below depicts the relationships between the theme, code, and responses.



**Figure 4.8 Information management**

In the figure above, the relationships between the theme and codes are displayed by means of a red dashed line. Furthermore, the relationships between codes and responses are displayed by means of a black arrow.

In closing, the company does not share personal information and it is not used for marketing purposes. Sharing of information is only done in compliance with regulations. Validation processes are in place and updates to these are being investigated. According to strategic management, all information captured electronically is verified through a business process, but slightly more than half of operational staff stated that they verify client email addresses. Additionally, it was found that users depend on information that is captured correctly and updated regularly. The data showed that even though the organisation manages its clients' personal information from a procedural perspective, operational staff do not always adhere to these procedures.

#### 4.7 Information privacy

This theme emerged from the empirical data and in this section all the findings are reviewed.

Clients can rest assured in knowing that information shared with the company will be protected and not shared with other parties for illicit or illegal purposes; thus, protecting information serves both the client and the company [AM]. The AM commented:

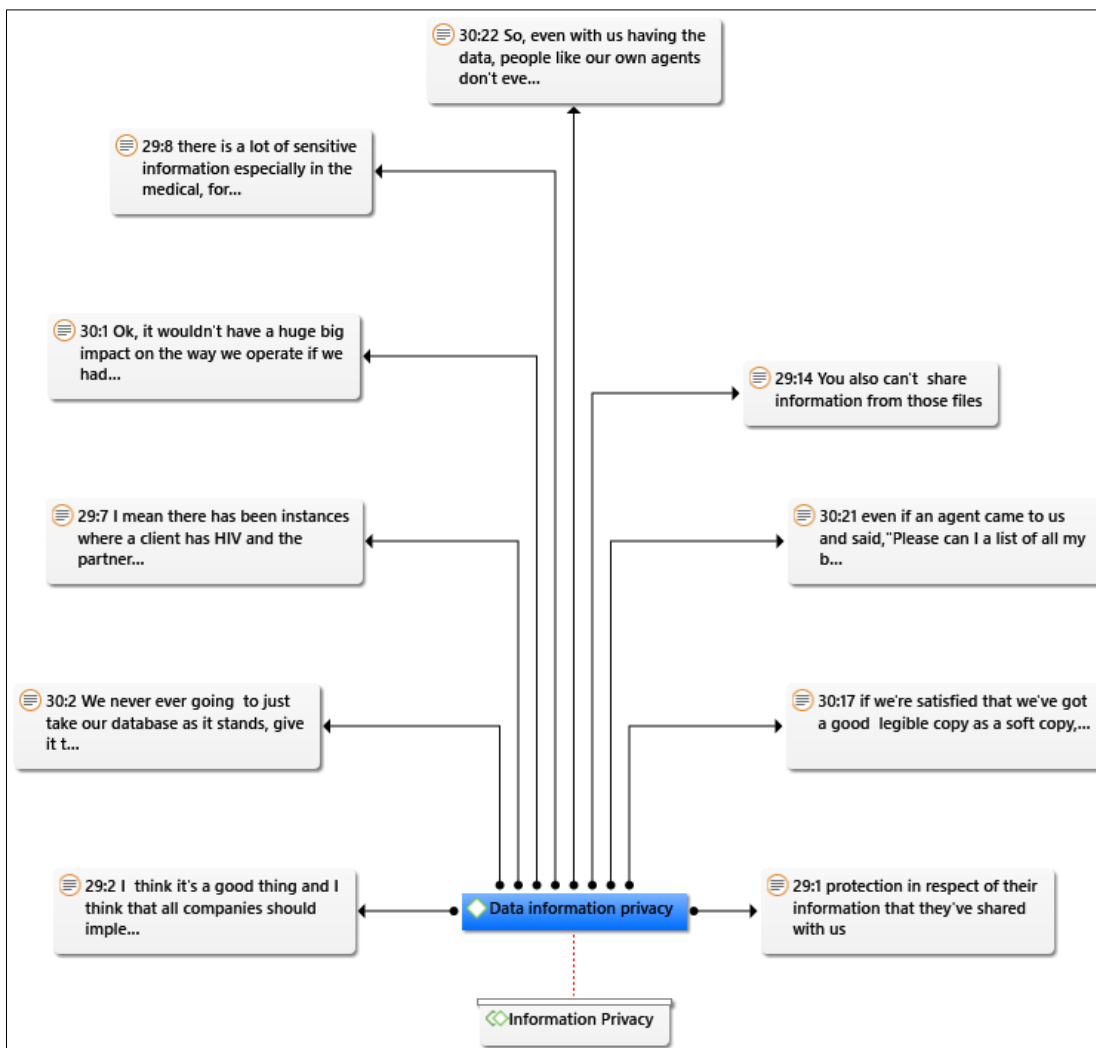
... protection in respect of their information that they've shared with us knowing that they're safe, knowing that they are not going to be exposed to some form of fraud or have their data exposed to these data companies that solicit information ...

In terms of direct marketing, the impact of POPIA on the business would be insignificant as the business does not share personal information and the database is never going to be used for marketing purposes [GM]. The GM commented:

OK, it wouldn't have a huge big impact on the way we operate if we had to make things any more stringent because we're not using data to sell to anybody, we're not giving data away.

Once all information is stored electronically, physical copies are destroyed [GM]. Information is shared only after it has been authorised and emphasis is on compliance with regulatory requirements [GM].

The network diagram overleaf illustrates the relationship between theme, code, and responses.



**Figure 4.9 Information privacy**

In the figure above, the relationships between the theme and codes are displayed by means of a red dashed line. Furthermore, the relationships between codes and responses are displayed by means of a black arrow.

In closing, the organisation emphasises the importance of adhering to requirements.

#### 4.8 Policies

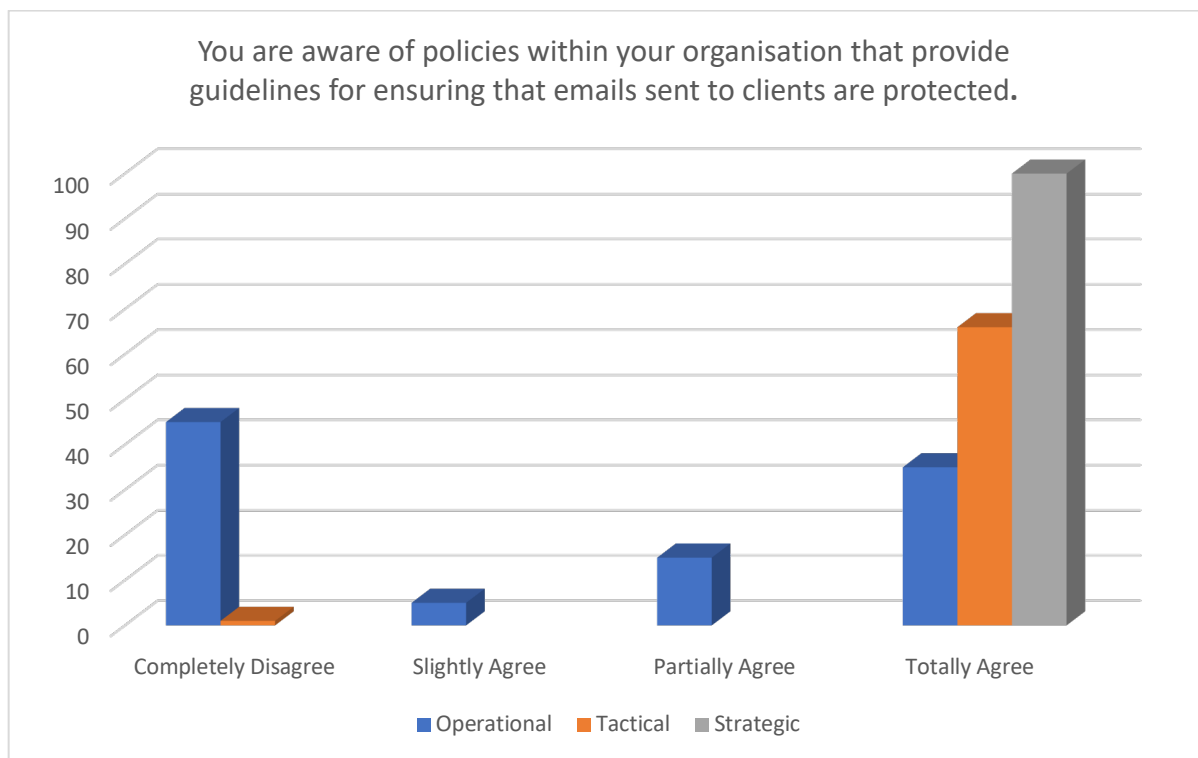
The theme 'policies' (2.4) emerged from the literature review. This section reviews the empirical data relating to this theme.

Provision had been made in company policy in terms of prohibiting the divulging of any information relating to the company or its clients [AM]. Staff are informed about what they may

share in terms of information [AM]. The risk management policies are reviewed annually to determine the impact that changes in legislation have on the business [GM]. POPIA has become part of this review [GM]. She commented:

... we have the company policy, the company handbook, which very specifically states that you cannot divulge any information from the company or any of its clients ...

The graph below displays responses to the statement: “You are aware of policies within your organisation that provide guidelines for ensuring that emails sent to clients are protected.” This statement is found in all three questionnaires. In questionnaire A and C, this was Question 1. In questionnaire B, this was Question 2.

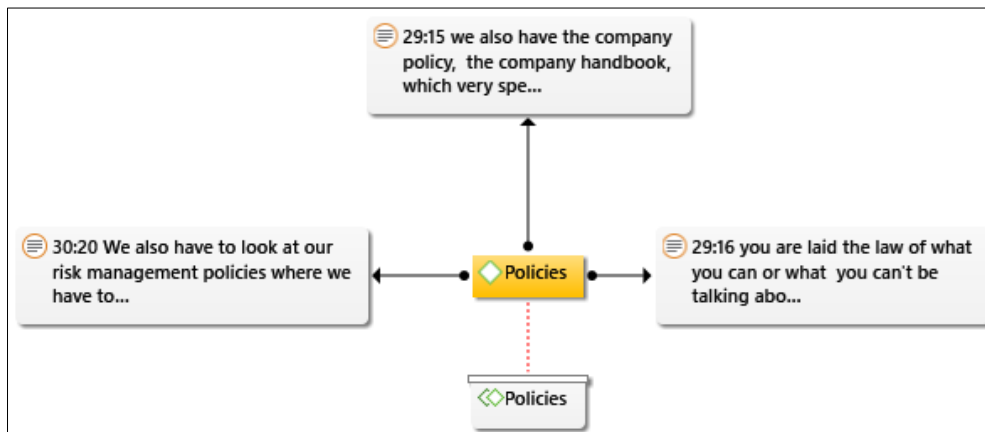


**Figure 4.10 You are aware of policies within your organisation that provide guidelines for ensuring that emails sent to clients are protected**

The strategic organisational level respondent totally agreed with the statement. One of the tactical level respondents completely disagreed, while two totally agreed. Slightly less than half of operational respondents completely disagreed with the statement: “You are aware of policies within your organisation that provide guidelines for ensuring that emails sent to clients

are protected.” The rest were distributed among ‘totally agreed’, ‘partially agreed’ and ‘slightly in agreement’ with the statement. Knowledge regarding the topic is questionable.

The network diagram below depicts the relationships between the theme, codes, the responses.



**Figure 4.11 Policies**

In the figure above, the relationships between the theme, codes, and responses are displayed. For example, quotation 30:20 links directly to the code ‘policies’.

In closing, responses from the tactical level revealed that information privacy is provisioned under the company policy. The strategic point of view indicated that annual reviews are conducted to assess changes in legislation and the impact of such changes on the business. However, the operational level survey responses indicated a difference of opinion regarding awareness of such policies.

#### **4.9 Reasons for compliance battle**

Reasons for compliance battle is another category that emerged during analysis.

This section reviews the sub-categories which are:

- Archived and backed-up data (4.9.1)
- Outdated methods (4.9.2)
- Hard copies (4.9.3)
- Vague requirements (4.9.4)
- Skills/Training (4.9.5)



#### **4.9.1 Archived and backed-up data**

Deletion of emails that contain personal information can become an extensive exercise [ITST].

The ITST commented:

That's going to be a bit of an issue because most of our emails get archived for five years as well; erm, to go through all of those to delete every single mail from that specific person is gonna take quite a long time to do, so yeah, that will be a bit of a headache, a lot of work hours to get them totally off your environment.

Large amounts of personal information are included in the data that gets backed up frequently, and as a result, removing data from backups can be extremely problematic [ITST]. The ITST commented:

Look, to go through all the backups, so, if we have to delete information from the backups it means that we have to go through each and every backup of the last five years and then the monthlies as well to go and search for that as well to go and search for that because if you take for instance, if you have a monthly backup and that guy started in January and in December he decides, "OK, I want all my information removed," we have to go through from December backwards each and every tape to remove all this information.

#### **4.9.2 Outdated methods**

Working with a piece of paper is not always practical. Faxing and printing do not fit in this century and doing things via the post office is considered obsolete [AM]. The AM commented:

Well, you have made me aware of it now that there is a form that needs to be completed. I don't know necessarily that we're aware of that actual form being utilised here in the business; we usually just put something in writing from the client and confirmation on the telephone that they will be sending something via email. I do not know in the bigger scope of things in that type of marketing environment getting a piece of paper to a person to sign. It is like me going to the police station and asking for, you know, or somebody asking for an affidavit.

#### **4.9.3 Hard copies**

Dealing with hard copies could pose a threat and could prove to be more challenging [GM]. Hard copies were not necessarily stored according to a filing system and if they had to retrieve such information, it would be costly [GM]. Information was stored long before any information

protection or retention Acts were promulgated and [I] was wondering whether these factors were considered when these laws were drafted [GM]. Going forward, no information would be sitting in storage facilities; however, historical information will still exist in storage and expunging that information could be an impossibility [GM].

So hard copies pose more of a threat, in my mind. So, we have agents that work all over the country. They go out, they meet with the client. They then get that piece of paper, scanned into us but they still sit with the original copy.

#### **4.9.4 Vague requirements**

The interpretation of POPIA is still wide open, while other international Acts are very clear as to their requirements [GM]. The GM commented:

... specific the Act is in Canada and the states, sorry I forget the names, but that we're at that same level, that there's no concern about how they're open to interpretation, that they're actually so fastidious in the policy wording that there's no leave to apply it as you want to.

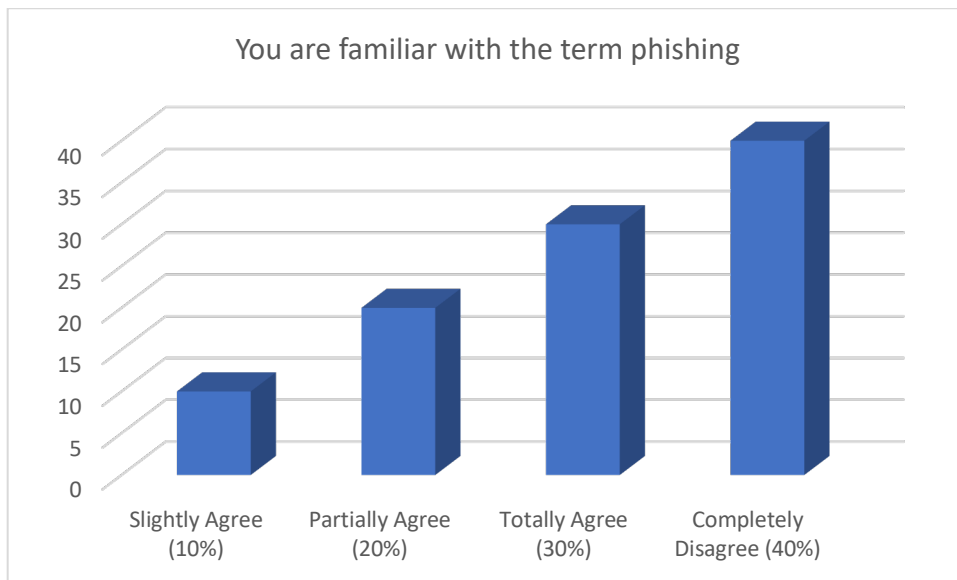
#### **4.9.5 Staff and skills training**

Staff training is important and empowering staff in terms of computer and information security is essential to ensure that the company operates in a manner that is consistent with the requirements of POPIA [AM]. The AM commented:

... it is important to train staff as well not to disclose just anything either.

Graphically represented overleaf are the responses to the statement:

"You are familiar with the term 'phishing'."

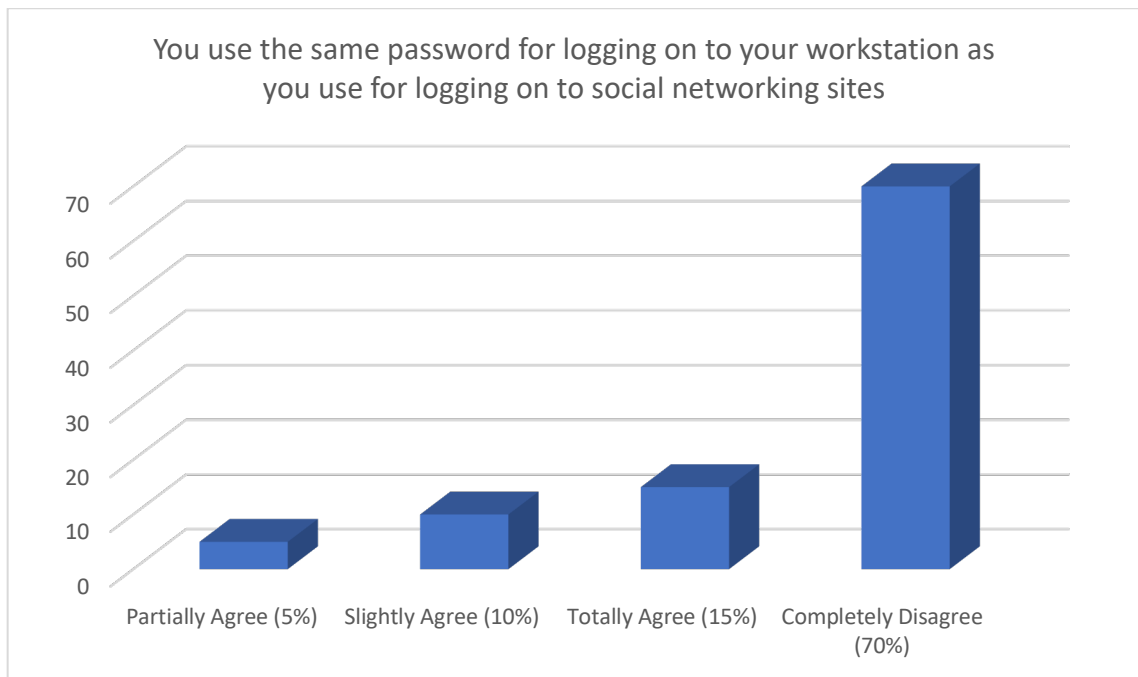


**Figure 4.12 You are familiar with the term ‘phishing’**

Forty percent of respondents stated that they were completely unaware of the term ‘phishing’, 30% were completely aware, 20% were partially aware and 10% were slightly aware.

Only 30% of respondents were familiar with the term ‘phishing’ and 70% of respondents were slightly, partially and completely unfamiliar with the term.

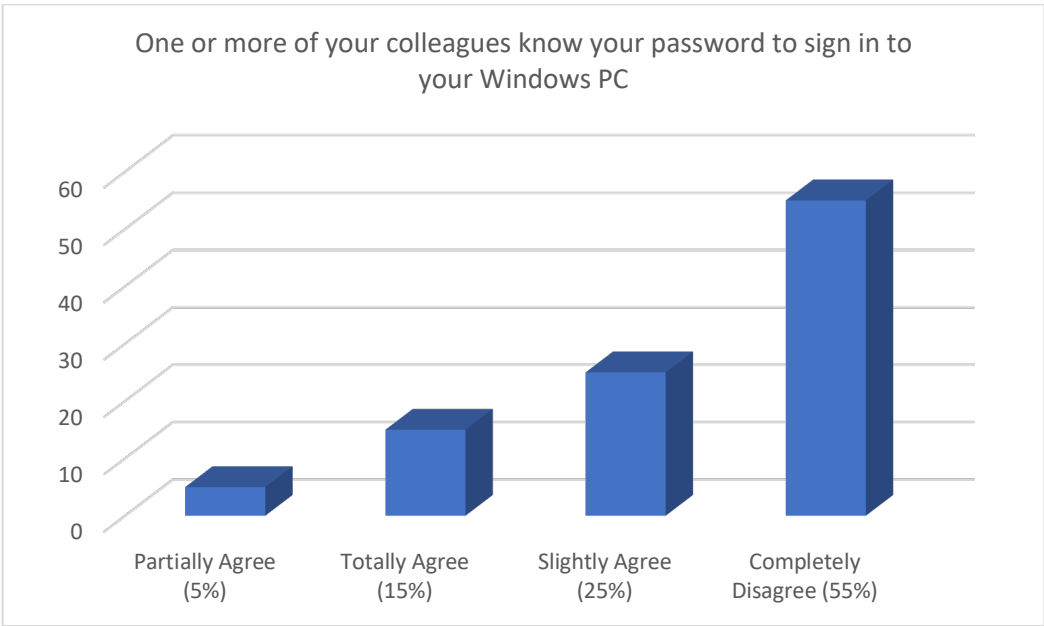
In the graph overleaf, the responses to the statement, “You use the same password for logging on to your workstation as you use for logging on to social networking sites” is presented.



**Figure 4.13 You use the same password for logging on to your workstation as you use for logging on to social networking sites**

More than half of respondents, 70%, disagreed with the statement. Other responses were distributed among the 'partially', 'slightly' and 'totally agree' scales.

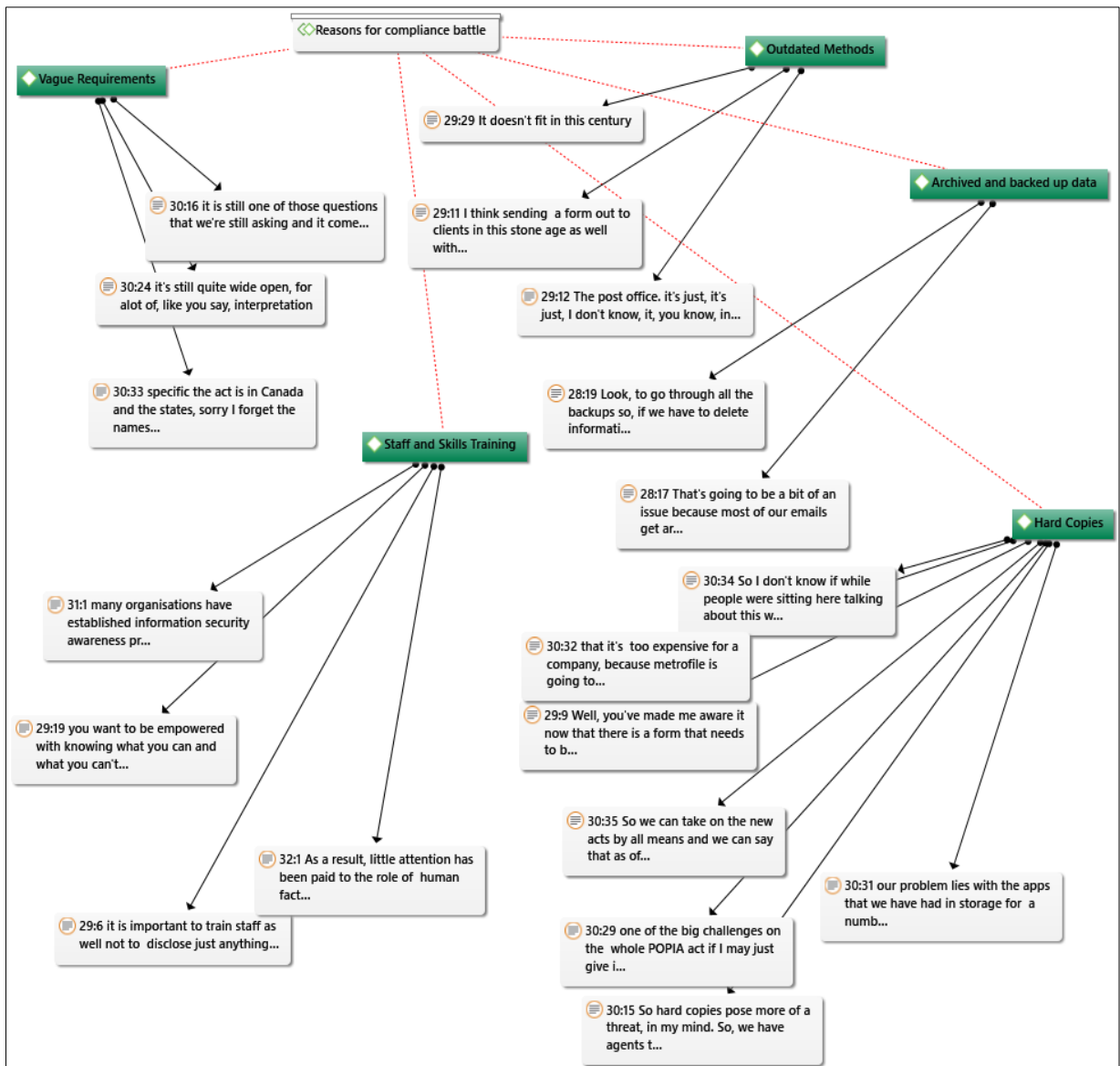
The graph overleaf illustrates the responses received from operational staff to the statement: "One or more of your colleagues know your password to sign into your Windows PC."



**Figure 4.14 One or more of your colleagues know your password to sign into your Windows PC**

Slightly more than half of the respondents (55%) do not share their passwords with colleagues, whereas the remainder do. Further responses indicated that IT staff are aware of users' passwords.

The network diagram overleaf depicts the relationships between the theme, codes, and responses.



**Figure 4.15 Reasons for compliance battle**

In the figure, the relationships between the quotations and codes are displayed by means of a red dashed line. Furthermore, the relationships between codes and responses are displayed by means of a black arrow. The quotations are linked to the relevant themes.

In closing, the operational perspective indicated that emails and data are backed up and stored for five years and removing specific information can be a very cumbersome exercise. From a tactical point of view, it was indicated that working with paper-based documents and using faxes and the post office are impractical in this modern-day society. The strategic level pointed out that data protection law is new in South Africa and that managing with archived paper-backed information could result in financial loss. In addition, the strategic level also stated that

POPIA is vague in its requirements. Through the lens of the operational level, it was found that staff were not familiar with common hacking techniques.

#### **4.10 Technical measures**

The theme 'technical measures' (2.5) emerged from the literature review. POPIA requires reasonable technical measures be put in place to safeguard personal information. Computer systems are composed of two types: hardware and software. The responses were grouped into the same categories because the responses were linked to either hardware or software.

Therefore, this section reports on the two logical categories below:

- Hardware protection (4.10.1)
- Software protection (4.10.2)

The next section discusses hardware protection.

##### **4.10.1 Hardware protection**

After implementation, the firewalls are examined to ensure they are up to standard and annual penetration tests are conducted by external companies [ITST]. The ITST commented:

... first of all, we must make sure that our firewall implementation is up to standard so that nobody can go out from the inside.

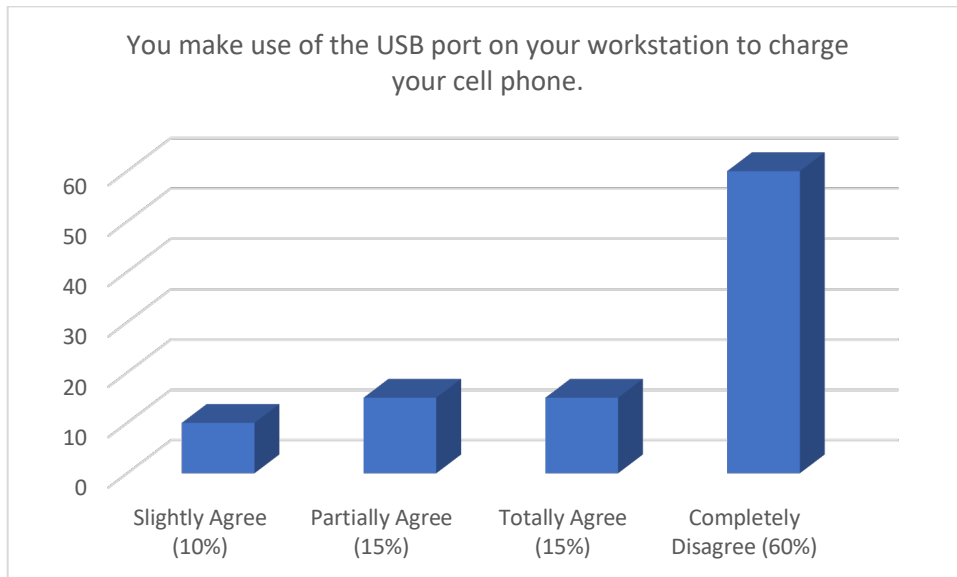
Access to USB ports on all workstations was prohibited as a protection method against viruses that could enter the internal network and all USB connections to PCs were blocked [ITST]. The ITST commented:

... we did it to make sure that nobody can put a USB stick into their desktops or laptops to copy or bring other naughty little things onto the network.

Guests are not allowed to connect to the network because of security reasons and because of the type of information that is stored [ITST]. The process of implementing a separate guest network to allow guests to connect but with different IP addresses, subnets and gateways as a security measure has begun [ITST]. MAC-related authentication will be introduced to ensure that only a set of known devices can connect to the network infrastructure, as the current setup

leaves room for exploitation [ITST]. An IT audit was conducted by an external company to check the level of security of the company's IT [GM].

The responses to the statement, "You make use of the USB port on your workstation to charge your cell phone," found in Questionnaire B, Question 6, are shown in the graph below.

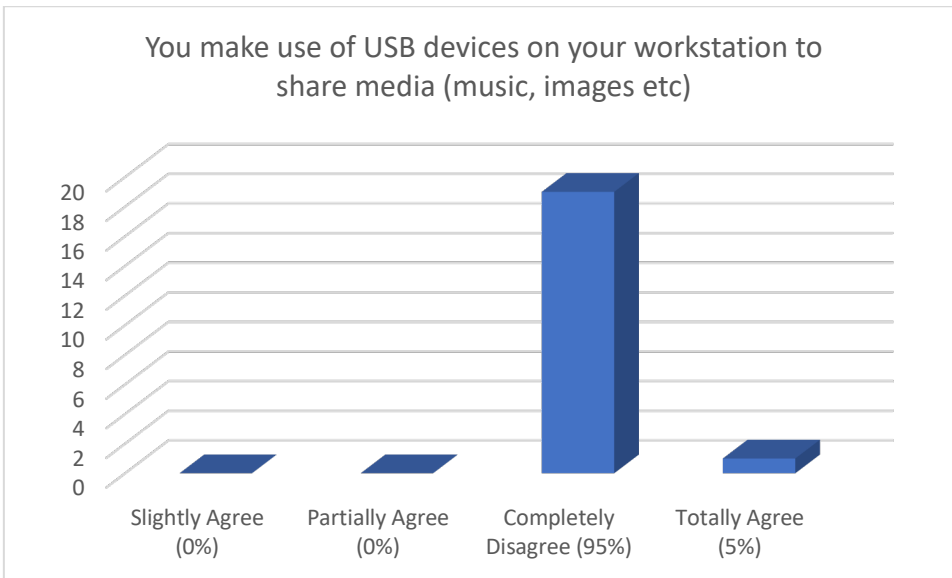


**Figure 4.16 You make use of the USB port on your workstation to charge your cell phone**

Most of the respondents completely disagreed, while only a few were in total agreement with the statement. From these results we can infer that some users might still be putting the organisation at risk.

The responses to the statement, "You make use of USB devices on your workstation to share media (music, images, etc.)," found in Questionnaire B, Question 8, are graphically represented overleaf.





**Figure 4.17 You make use of USB devices on your workstation to share media (music, images, etc.)**

An overwhelming number (95%) of respondents were in complete disagreement with the statement, whereas only a single respondent was totally in agreement. From these results we can infer that the majority of respondents act in accordance with company policy regarding the use of USB devices.

#### 4.10.2 Software protection

As a best practice, frequent password changes are enforced [ITST]. He stated:

... we follow best practices of users changing passwords every three months, which comes up that prompts you to change it, that's the one thing that we do ...

To enhance the security, firewalls were configured to allow only a certain set of external IP addresses to connect to the network [ITST]. The IT support technician commented:

... what I've done so far on the firewall is to allow only their external public IPs to get into our network, so if you're not part of that group you can't get into our network from the outside.

Sophos antivirus is installed on all the servers as this software has an additional protection measure to prevent its uninstallation [ITST]. He commented:

I implemented Sophos antivirus on all the servers which you cannot uninstall without a proper code, so no ...

All desktops make use of the ESET® NOD32 antivirus program [ITST]. All emails are received via Securicom, which scans the content of the emails, including the HTML and links contained within the email [ITST]. The IT support technician stated:

... all emails are going through Securicom, which gets scanned before it gets delivered to us. They scan all HTML, http websites, all links that are on there. And in fact, I actually stopped it.

Zip files are not allowed to be delivered via email as this is a common attack used by hackers to compromise systems. These files have names like 'photos.zip', thus fooling a recipient into believing that it is safe to open [ITST]. He commented:

... we don't allow any zip files to come through, that only because some hackers do attempt to put ransomware in zip files and call it photos.zip and a user think hey, it's my friend that send it to me and then it opens a whole can of worms ...

Only certain users are granted access to certain types of information [AM]. The administration manager stated:

... there are certain controls where only certain staff are able to view certain information ...

The login password management has been improved [GM]. She stated:

... the password login wasn't quite as strictly managed as it is now ...

It is of utmost importance that passwords should be updated frequently [GM]. The general manager said the following:

So, first of all there has to be a password for access and secondly those passwords have got to be updated on a regular basis.

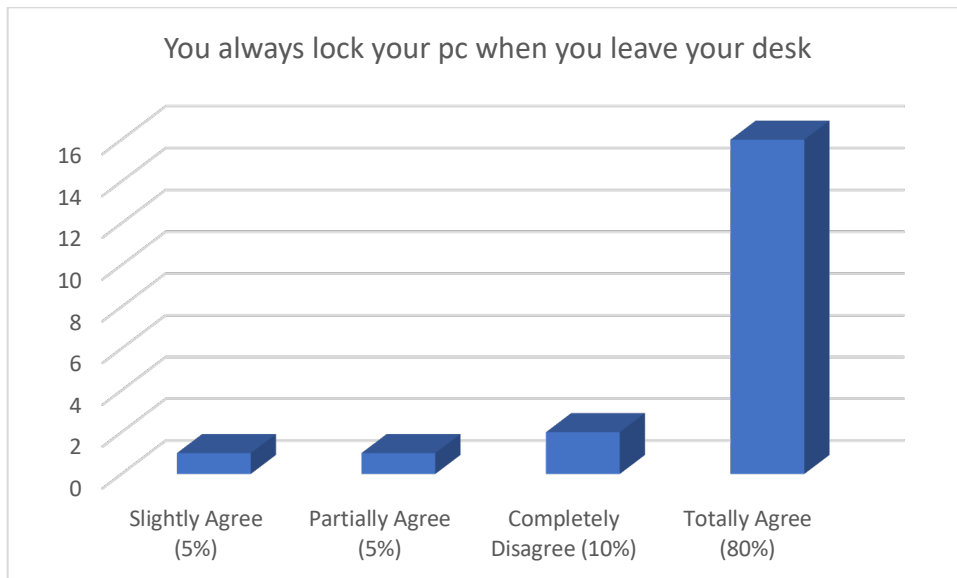
Database protection, as well as firewalls, are in place [GM]. Files are protected on the server by means of a firewall, protected access and password control [GM]. She commented:

We've obviously then got protection on our database, we've got firewalls in place, so we shouldn't have people coming in and being able to steal the data.

Investigation into the implementation of additional security measures in terms of mobile email access has already begun [ITST]. The IT support technician stated:

... the files, you know, sit on our main server, with a firewall, protected access and password control.

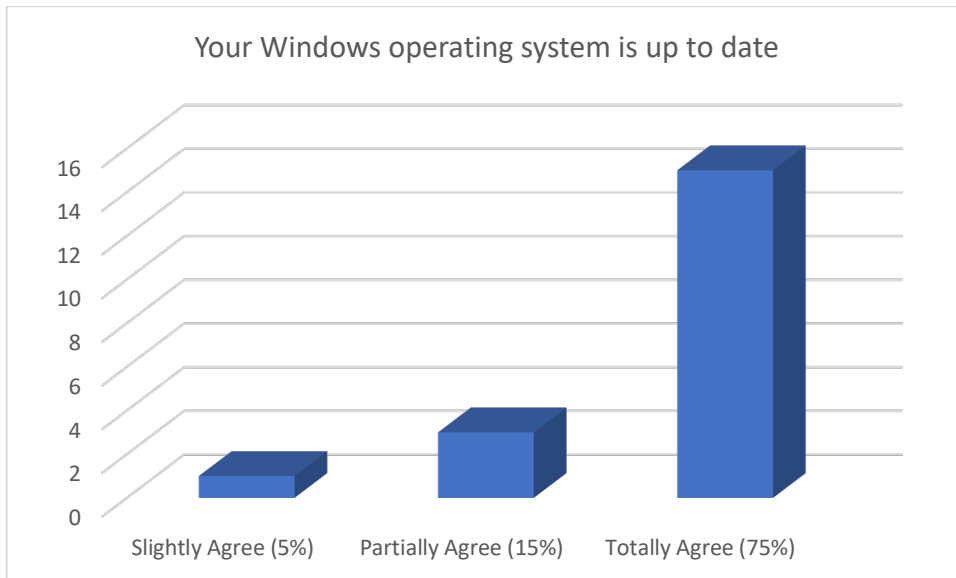
Results from Questionnaire C's (Section 3.11) statement, "You always lock your PC when you leave your desk," which was presented to operational staff, are represented graphically below.



**Figure 4.18 Always locks PC when away from desk**

The majority (80%) of staff indicated that they fully agreed with the statement. Very few either partially, slightly or completely disagreed. From these results we can infer that most users act in accordance with company policy.

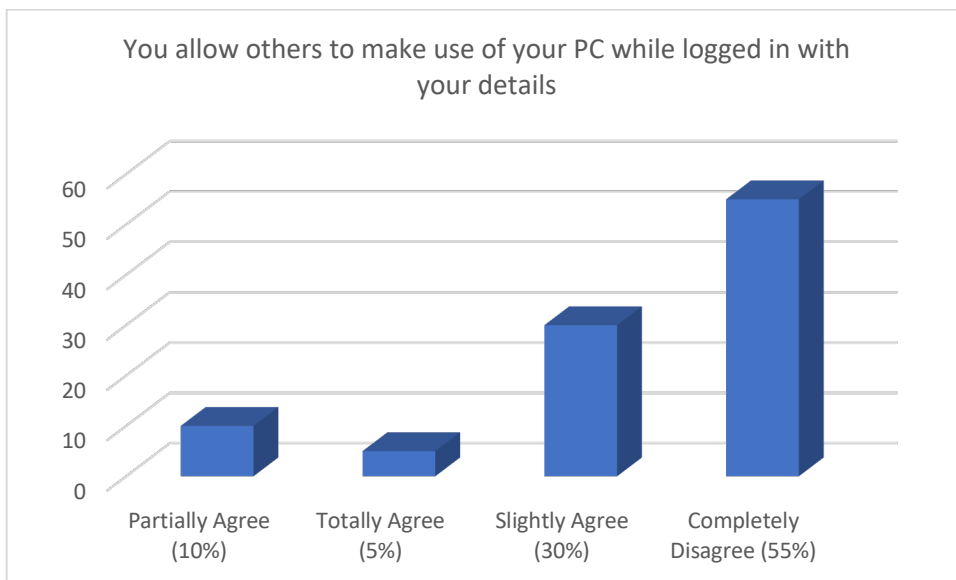
The results from the statement, from Questionnaire C (Section 3.11), "Your Windows operating system is up to date," are presented overleaf.



**Figure 4.19 Windows operating system is up to date**

Most (75%) respondents totally agreed with the statement. Some (15%) were in partial agreement with the statement and only one slightly agreed. One of the responses did not select an option.

In the graph below, the responses from operational staff to the statement, “You allow others to make use of your PC while logged in with your details,” are depicted.



**Figure 4.20 You allow others to make use of your PC while logged in with your details**

A little more than half (55%) of operational staff completely disagree with the statement. However, 5% percent do, 30% are in slight agreement and 10% partially agree. From these results we can infer that there is no threat perceived by operational level respondents in sharing PCs with colleagues while logged in.

The network diagram below depicts the relationships between the theme, codes, and responses.

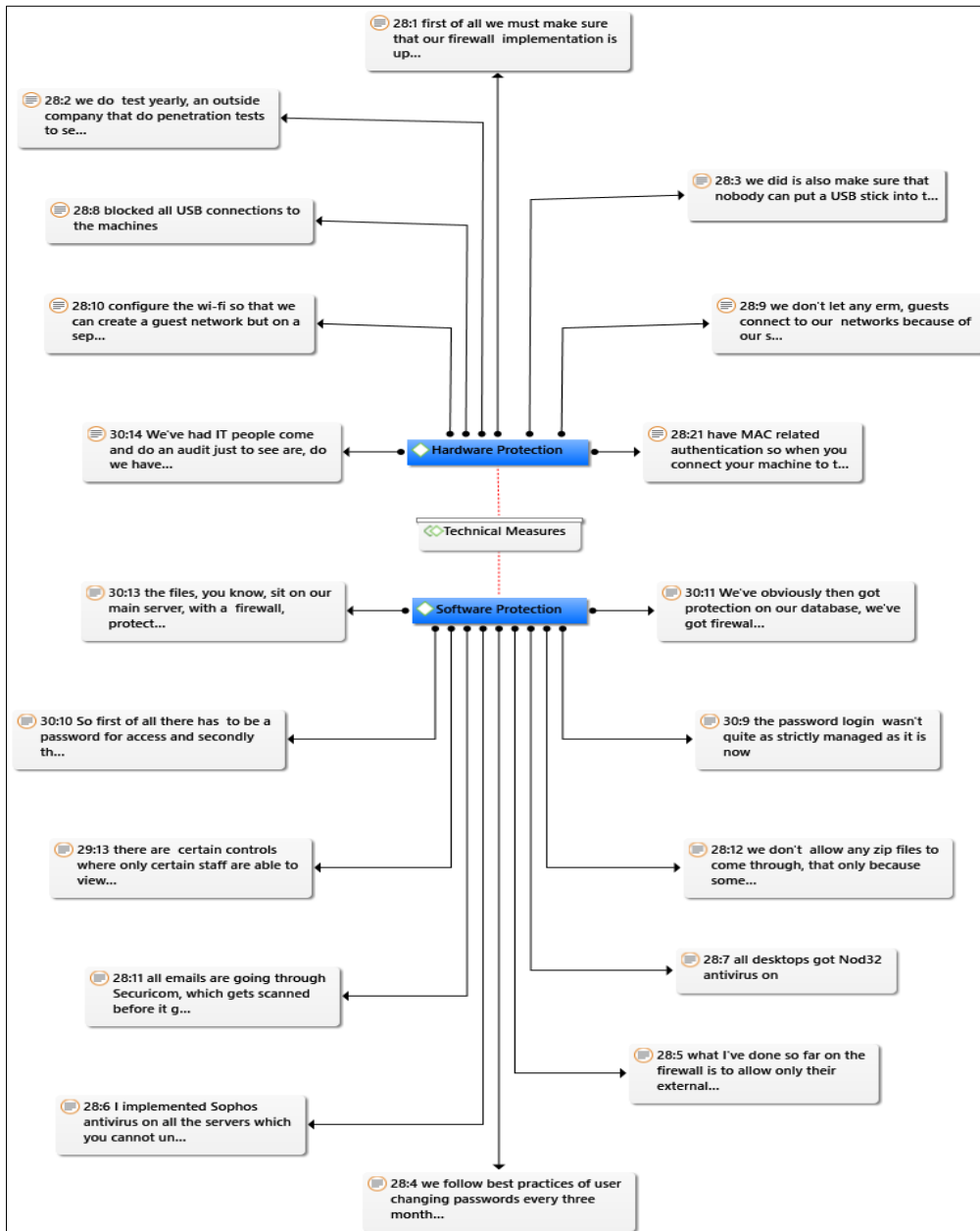


Figure 4.21 Technical measures

In Figure 4.21, the relationships between the theme and codes are displayed by means of a red dashed line. Furthermore, the relationships between codes and responses are displayed by means of a black arrow.

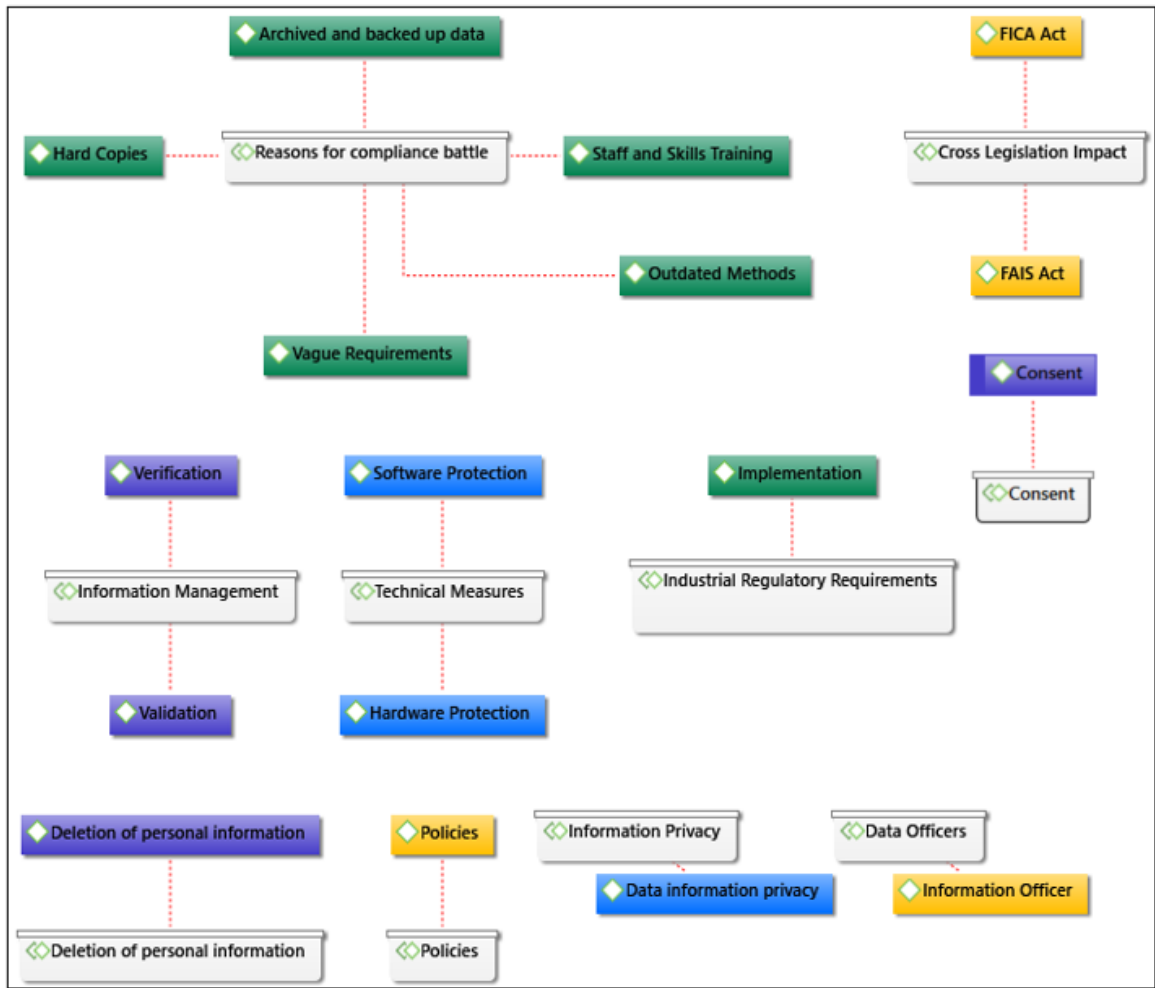
In closing, the technical expertise was obtained from the ITST from the operational level within the organisation. Hardware and software security measures were implemented but the analysis of the survey results indicated that operational staff still act in a manner that could jeopardise such implementations. The strategic level stated that IT audits were conducted, which could be interpreted in a way that suggests IT security is a priority of the organisation. In addition, the strategic perspective also stated that security enhancements had been done recently. The responses from the tactical level indicated some knowledge about access control management.

#### **4.11 Summary**

In closing, the data has highlighted several challenges faced within the organisation. One of the most pertinent is that staff lack knowledge in respect of protecting information. It was found that the majority users are not familiar with common hacking techniques which puts the company at risk of cyber-attacks. A previous study found that higher cyber knowledge is linked to the cyber awareness level of participants (Zwilling et al., 2020).

The data has highlighted issues relating to conflicts between POPIA and other legislations. It was recommended in another study that the Health Professions Council of South Africa should align its guidelines with other legislation like POPIA by incorporating its provisions to protect practitioners (Van Niekerk, 2019).

The network diagram overleaf depicts the relationships between all the themes covered in this chapter.



**Figure 4.22 Themes and codes**

Figure 4.22 shows the codes that emerged during analysis and the links to the themes. The codes relating to a specific theme were grouped accordingly. The figure excludes quotations. **Consent** (4.1) consists of a code based on quotations relating to issues of consent. POPIA is not a consent driven law and is only required in certain scenarios.

**Cross-legislation impact** (4.2) emerged from analysis and consists of codes based on contradictions between POPIA and other legislation. The study highlighted contradictions found between FAIS and FICA and POPIA.

**Data officers** (4.3) consists of one code comprising responses to the benefits and challenges relating to the designation of information officers. The importance of having designated information officers has been highlighted by analysis and literature. POPIA's subjective impact will require an information officer in every business and sector.

**Deletion of personal information** (4.4) consists of a code based on factors that hamper efforts to delete information. Data pointed out that the organisation was able to meet requests from clients to have their information removed. Big tech companies like Google had a few legal battles that ended up being costly (2.3.1).

**Industrial regulatory requirements** (4.5) consists of a code based on the implementation of regulatory requirements. Data showed that the organisation had additional regulatory requirements that they had to abide by, thus creating a grey area where POPIA is concerned.

**Information management** (4.6) comprises codes based on procedures implemented to validate and verify information. POPIA requires that personal information be kept up to date and accurate. The organisation had verification and validation processes in place that ensures information accuracy.

**Information privacy** (4.7) consists of a code based on the role privacy plays within the organisation. Analysis showed that information privacy enhances trust with consumers.

**Policies** (4.8) consists of a code based on policies within the organisation. It emerged from analysis that policies put in place are not always adhered to. This could be for a variety of reasons. Nevertheless, all role players should be aware of information protection policies.

**Reasons for compliance battle** (4.9) consists of codes based on compliance barriers. These barriers were the difficulty of working with backed-up data, working with outdated methods or systems, issues with paper-based information, POPIA's vague requirements, and staff cyber security awareness levels.

**Technical measures** (4.10) consists of two codes. These codes were based on hardware and software protection measures. It emerged from analysis that technical measures, relating to hardware alone, are imperative in protecting against threats. In addition, software protection measures were put in place as well.

In the next chapter, conclusions and recommendations are presented.



## 5 CHAPTER FIVE: CONCLUSIONS AND RECOMMENDATIONS

*“Everyone can rise above their circumstances and achieve success if they are dedicated to and passionate about what they do” – Nelson Mandela*

In Chapter 4, the findings were presented. This chapter consists of the following sections:

- Chapter review (5.1)
- Revisiting the objective and research questions (5.2)
- Limitations of the study (5.3)
- Research Contributions (5.4)
- Recommendations (5.5)
- Future research (5.6)

This chapter closes with the section titled Finally (5.7).

### 5.1 Chapter review

A brief recapitulation of all the preceding chapters is given in this section. It commences with Chapter 1.

#### 5.1.1 Chapter 1 – Introduction

Chapter 1 identified the problem (1.1, 1.2) that companies have not yet started to prepare for compliance with POPIA and that guidelines for achieving compliance are limited. Furthermore, very steep fines of up to ten million rands can be imposed on companies for non-compliance. Additionally, Chapter 1 introduced the research questions and objectives (1.3), the aim (1.4), the rationale for the study (1.5), delineation (1.6), contributions of the research (1.7), and ethical considerations (1.8), and closed with a summary.

#### 5.1.2 Chapter 2 – Literature review

Chapter 2 reviewed the literature to gather theoretical data and to identify a gap in the literature. Emergent themes derived from literature sources drove the formulation of research questions posed in interviews and questionnaires. The themes are ‘consent’ (2.2), ‘data officers’ (2.3), ‘deletion of personal information’ (2.4), ‘policies’ (2.5) and ‘technical measures’ (2.6). Each theme comprised sub-sections that included GDPR, PIPEDA, DPA, POPIA and a crystallisation section.

### 5.1.3 Chapter 3 – Research design and methodology

Chapter 3 presented the research design (3.1) and research methodology (3.2). The research design included the philosophy, approach, methodological choice, time horizon, and techniques and procedures. The research methodology included sampling, data-collection methods, case description, unit of analysis, ethical considerations, trustworthiness, and delimitation. The respondents were grouped in a hierarchical structure and this organisational grouping impacted and guided the design of interview protocols and questionnaire instruments.

### 5.1.4 Chapter 4 – Findings and analysis

Chapter 4 incorporated a thematic analysis of the empirical data from both the interviews and questionnaires. New themes emerged during the analysis of the empirical data. The data was presented thematically.

## 5.2 Revisiting the objective and research questions

This section gives an overview of the research objective and research questions.

The mapping of the objective and research questions is displayed in the table below.

**Table 5.1 Research questions and objectives**

<b>Research Questions</b>	<b>Objectives</b>
<b>MQ What implementation guidelines should be considered by SMEs to promote compliance with POPIA?</b>	<b>MO Explore implementation guidelines that can be utilized by SMEs that can promote compliance to POPIA.</b>
<b>SQ1 What are current challenges that SMEs could face when implementing POPIA compliance?</b>	<b>O1 Explore what challenges SMEs could be faced with when implementing POPIA compliance.</b>
<b>SQ2 How can POPIA compliance implementation challenges be met?</b>	<b>O2 Explore how POPIA implementation challenges can be met.</b>

For the convenience of the reader, Table 1.1 from Chapter 1 is repeated.

This chapter answers the research questions and end with a summary.

### 5.2.1 What are current challenges that SMEs could face when implementing POPIA compliance (SQ1)?

This study highlighted various challenges:

- Adherence to policies
- Cross-legislation impact
- Cyber security awareness among staff
- Deletion of personal information
- Designation of information officers
- Direct marketing
- Paper-based information
- Reasonable technical measures

The figure below is a graphical representation of the links between SQ1 and the challenges identified:

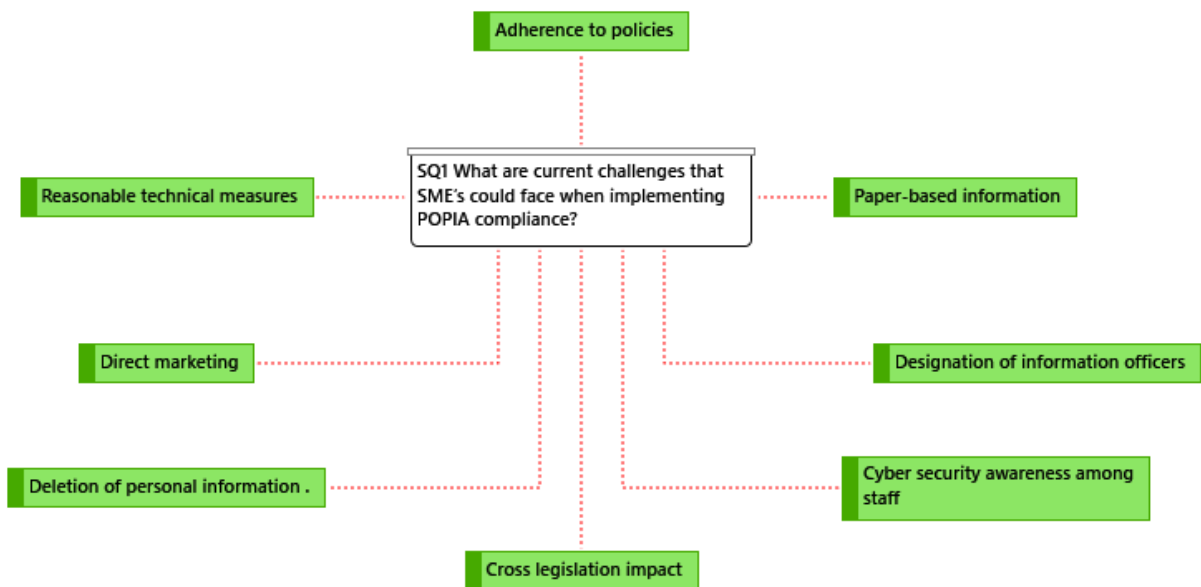


Figure 5.1 SQ1 and answers

As shown in Figure 5.1, the challenges identified were linked to the secondary research question, SQ1.

**Adherence to policies** emerged as a challenge. POPIA requires policies be put in place in companies with the purpose of protecting personal information (2.5.4). It has emerged from

data that according to strategic and tactical management, the organisation has put policies in place aimed at the protection of personal information (4.7). Again, a gap in the perceptions of strategic, tactical and operational levels about company policy was identified (Figure 4.2). The responses to the statement, “You are aware of policies within your organisation that provide guidelines for ensuring that emails sent to clients are protected”, indicated that slightly less than half of operational staff were in complete disagreement as opposed to strategic staff respondents who were fully in agreement with the statement.

**Cross-legislation impact** is a challenge that emerged from the data (4.3). POPIA grants individuals the right to have their personal information removed from where it is held in a data processor. On the other hand, there are laws like FICA (4.3.1) and FAIS (4.3.2) that require records be kept for up to five years. One of the reasons for retaining information is to combat fraud, but at the same time clients must be granted the right to have their personal information deleted.

**Cyber security awareness among staff** emerged from data as a challenge. Data has shown that operational staff are not aware of common hacking techniques (4.8.5). The responses to the statement “You are familiar with the term ‘phishing’” indicated that few respondents were in complete agreement with the statement (Figure 4.4). Furthermore, operational staff share their passwords with colleagues (Figure 4.6).

**Deletion of personal information** emerged as a challenge from both literature and empirical data. POPIA grants the right to individuals to request that their personal information be removed (2.4.4). It emerged from empirical data that deletion of personal information might not be possible in certain instances (4.5). Information that is backed up might not be easily accessible or easily mutable. It emerged from the data that a gap exists between the perceptions of strategic and tactical levels in terms of the organisation’s capability to carry out a request to have the personal information of an individual deleted in a timely and accurate manner (Figure 4.1). Furthermore, it emerged that from an operational perspective, deletion of personal information can become a very time- and resource-consuming exercise (4.5). It emerged from analysis that removing emails that contain confidential information can be a very cumbersome exercise also (4.8.1).

The **designation of an information officer** is a requirement of POPIA (2.3.4). Companies cannot appoint such individuals before POPIA comes into full effect (4.4). Furthermore, information officers need to be registered with the information regulator. The Act currently is

not in full effect, preventing the organisation from appointing an information officer. In addition, information officers need to be registered with the information regulator.

**Direct marketing** emerged from data. POPIA requires a form to be completed, in writing, by clients to obtain consent for the use of their personal information (2.2.4). It is odd that in contemporary sales strategies, written consent is required for direct marketing purposes.

**Paper-based information** emerged from empirical data as a challenge. It emerged from data that the AM (tactical level), believed that working with paper is in direct conflict with contemporary methods relating to running a business and its operations (4.8.2). It further emerged from analysis that the handling of paper-based information was not addressed or considered by POPIA (4.8.3). Additionally, the requirements of POPIA were vague, thus open to interpretation (4.8.4).

**Reasonable technical measures** are required to be implemented to protect personal information (2.6.4). POPIA fails to recognise or mention any technology that can assist in protecting personal information. It emerged from data that there are two aspects that form part of reasonable technical measures. these are hardware protection (4.10.1) and software protection (4.10.2). In terms of hardware protection, interviews with strategic, tactical and operational staff identified a similar level of understanding among organisational levels, although the depth of understanding varied considerably. A role player from the strategic level was aware of devices put in place to ensure network and data security, with no idea of how they work. The representative from the tactical level was only aware of controls put in place to ensure information security. However, the role player from the operational level was able to provide insight into the purpose as well as the detail surrounding these technical measures. It emerged that firewall installations require proper configuration coupled with penetration tests conducted by external companies to ensure a high standard of protection. Furthermore, the blocking of access to USB ports was implemented as a standard to curb staff from possibly spreading malware. Although the results from a statement in the questionnaire (Figure 4.8) indicated that staff do not make use of USB devices to share media, results from another statement (Figure 4.7) indicated that slightly less than half of staff do make use of USB ports to charge their cell phones.

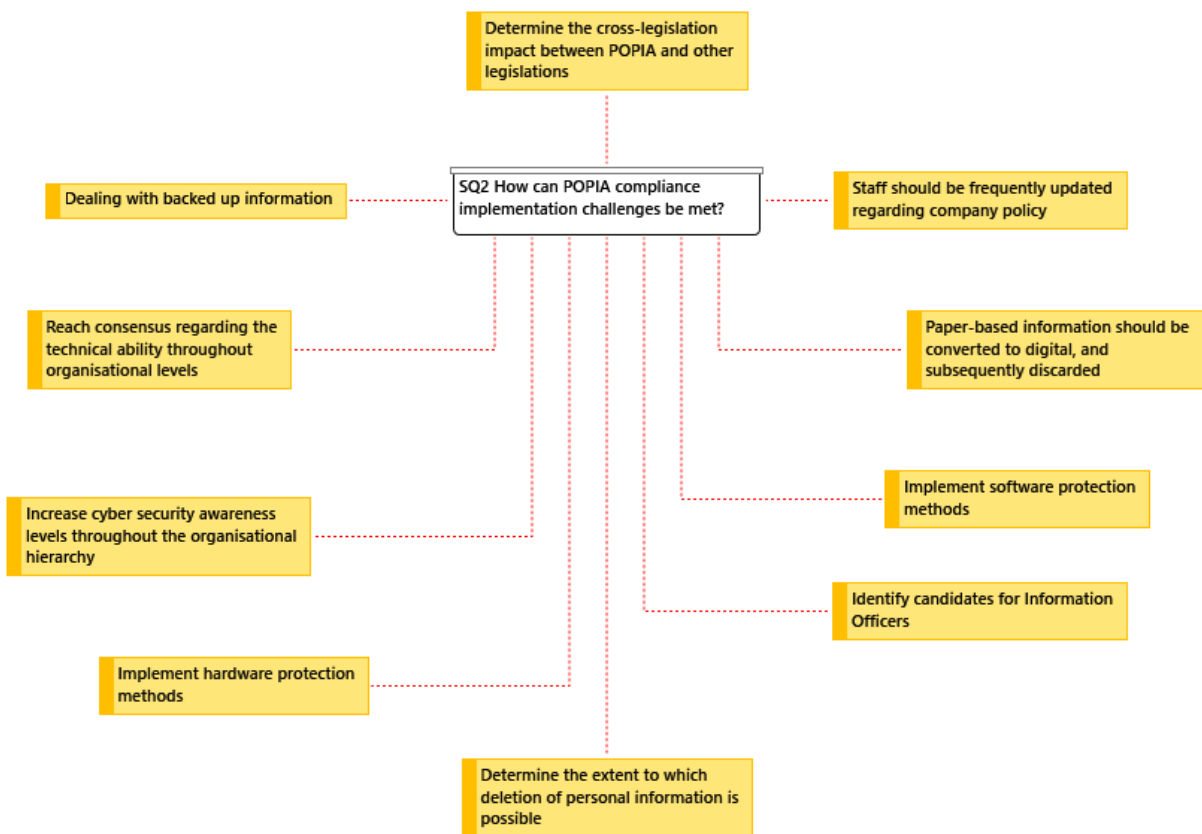
In the next section the secondary research question is addressed.

## 5.2.2 How can POPIA compliance implementation challenges be met (SQ2)?

Answering this question depended on the answering of **SQ1** in Section 5.2.1. This section responds in terms of challenges identified, with a list of actions that can be performed to meet these challenges. These actions are listed below:

- Deal with backed-up information.
- Determine the cross-legislation impact between POPIA and other legislation.
- Determine the extent to which deletion of personal information is possible.
- Identify candidates for information officers.
- Implement hardware protection methods.
- Implement software protection methods.
- Increase cyber security awareness levels throughout the organisational hierarchy.
- Convert paper-based information to digital format and then discard paper records.
- Reach consensus regarding technical ability throughout organisational levels.
- Update staff frequently regarding company policy.

The figure overleaf is a graphical representation of the links between SQ2 and actions to be taken to meet the challenges.



**Figure 5.2 SQ2 and answers**

This section reviews the items displayed in Figure 5.2.

***Deal with backed-up information.*** When it comes to dealing with backed-up information, deletion was identified as a challenge (5.3.1), the main reason being the time and resources required. Therefore, companies should start reviewing back-up strategies within the organisation to determine exactly what would be required when the need to remove information arises. Furthermore, the extent to which deletion is possible should be identified and documented.

***Determine the cross-legislation impact between POPIA and other legislation.*** SQ1 revealed that cross-legislation impact is a major challenge that companies could be faced with (5.2.1). POPIA itself does not mention how to address this issue and does not state which legislation takes precedence over the other. Therefore, companies should determine exactly which legislation they need to abide by and contact the relevant legal departments for advice.

***Determine the extent to which deletion of personal information is possible.*** The right to deletion of personal information is granted to individuals by data protection legislation in

multiple countries (2.4.1, 2.4.2, 2.4.3, 2.4.4). Answers to **SQ1** revealed that deletion would be challenging in certain circumstances (5.3.1). A response from an interview indicated that masking and deletion are similar (4.5). As pointed out in the literature, masking can be used to protect personal information (2.6.5). Therefore, when deletion of personal information is not possible, masking of such information should be considered as an alternative.

**Identify candidates for information officers.** Another challenge revealed in answering **SQ1** is that information officers cannot be designated as the Act has not yet come into full effect. Companies should not see this as a reason to delay this designation. As pointed out by literature (2.3.4), companies should consider individuals that are familiar with the legal requirements that fall within the ambit of the organisation. This would increase the efficiency and effectiveness of dealing with POPIA-related issues. Therefore, the identification of possible candidates should commence as soon as possible.

**Implement hardware protection methods.** In terms of hardware protection, securing infrastructure like local area networks, requires a great deal of equipment coupled with the relevant expertise. The installation of network security devices like firewalls requires configuration that provides another level of protection and is considered essential. Furthermore, these firewalls should undergo penetration testing to ensure security is of a high standard. Allowing guests or visitors access to the organisation's wireless network should be avoided. This can be achieved by creating a separate guest network to provide wireless network access to visitors that require an internet connection and should be considered as it minimises threats to the main local area network. A threat to technical security measures was identified as risky behaviour by operational staff. Therefore, operational staff should be informed of the dangers associated with USB devices.

**Implement software protection methods.** In terms of software protection, password management should be in place. Hashing of passwords is a one-way method of encryption, which means it is almost completely undecipherable (Ah Kioon, Wang, & Deb Das, 2013). The effectiveness of hashing passwords can be significantly improved by combining it with additional measures (Farawn, Rjeib, Ali, & Al-Sadawi, 2020). It emerged from data that staff share workstations with others while logged in as themselves (Figure 4.11). Again, actions by operational staff were identified as high risk. Therefore, operational staff should be informed of cyber security. Access control measures should be put in place to ensure that the correct staff members have access to privileged information. Reputable anti-virus applications should be installed on all computers in the organisation. Email providers like Securicom should be



considered as they provide in-depth email scanning to check for possible threats. An easy way for hackers to enter a system is via email, thus a reputable email service provider should be used.

***Increase cyber security awareness levels throughout the organisational hierarchy.*** It was identified that operational staff act in ways that could jeopardise the effectiveness of technical measures put in place to secure computers and protect personal information. Literature has indicated that uninformed behaviour by staff could put IT infrastructure at risk. The results of the questionnaire indicated that operational staff were not aware of the term 'phishing' (Figure 4.2), which is a common attack used by hackers to enter secure systems. Therefore, companies should invest in upskilling not only operational staff but all staff, and improving awareness levels of cyber threats. This could be done by having frequent presentations and workshops as new cyber threats emerge almost daily.

***Convert paper-based information to digital format and then discard paper records.*** Companies in South Africa existed long before the POPIA Act was signed into law in 2013. Companies stored information in paper format and did not necessarily store records in a manner that allowed for easy retrieval. In the context of the organisation in this study, the company has paper-based information dating back as far as 2003 held in storage. This information is protected; however, meeting a request for deletion can become a costly exercise. Companies should investigate ways to retrieve these documents, determine whether they are still required, then, and where possible, create digital copies and discard the paper-based documents. The Fourth Industrial Revolution is upon us and therefore companies should start moving towards a digital approach in terms of information management and retainment.

***Reach consensus regarding technical ability throughout organisational levels.*** A gap in perception was identified between strategic and operational staff in terms of technical abilities. The strategic level was fully confident that the organisation could handle a request for deletion swiftly and accurately. An interview with the ITST, a role player from the operational level, revealed that it would not be quite as simple as perceived by strategic role players. It is evident that there are two contradictory views. The opinions among tactical role players were different. Strategic role players might be divulging information that is incorrect, information that could land them in hot water at a later stage. Therefore, discussions between operational, tactical, and strategic role players should commence to gain a better understanding of information technology capabilities. There should be a uniform perception of IT capabilities.

**Update staff frequently regarding company policy.** A gap was identified between the strategic and operational staff in respect of policy adherence. Strategic staff were fully aware of policies to protect information, but operational staff did not always adhere to these policies. Therefore, additional control measures should be put in place to ensure that operational staff act in accordance with company policies in terms of data and information protection. Furthermore, staff should be offered frequent workshops that inform them of the importance of acting in accordance with policy, with emphasis placed on information security.

### **5.2.3 What implementation guidelines should be considered by SMEs to promote compliance with POPIA (MQ)?**

To approach and solve this problem, two secondary questions were developed with the intent to identify what challenges will be faced when seeking POPIA compliance and what can be done to assist in overcoming or meeting these challenges. To answer the main research question, answers to the secondary questions were required. SQ1, answered in Section 5.2.1, is as follows:

What are current challenges that SMEs could face when implementing POPIA compliance?

SQ2, answered in Section 5.2.2, is:

How can POPIA compliance implementation challenges be met?

The objectives linked to the secondary questions have been met.

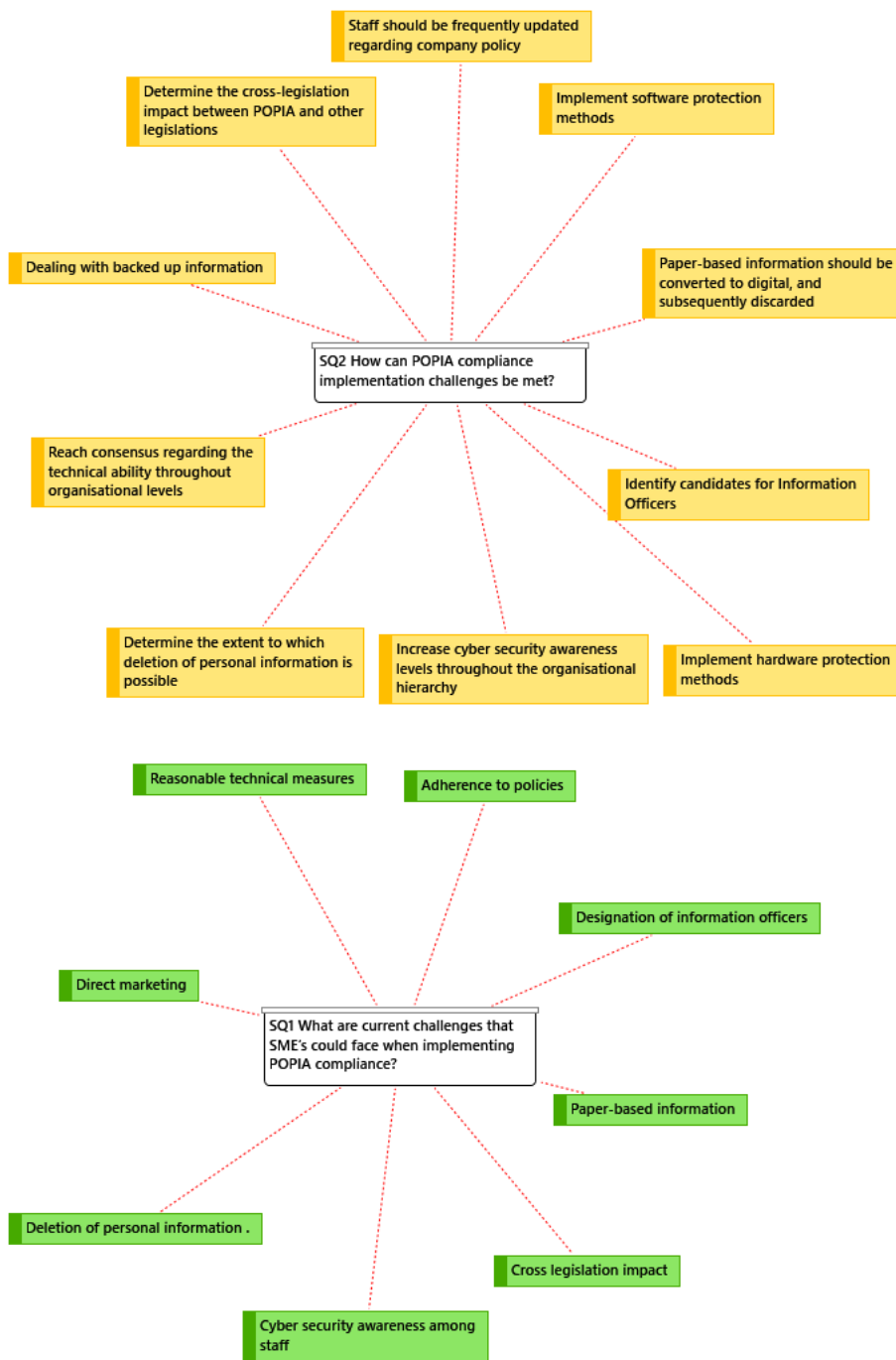
The study was directed by the main research question, MQ, as follows:

What implementation guidelines should be considered by SMEs to promote compliance with POPIA?

The identification of challenges and ways to meet these challenges formed the crux of the research and was therefore the primary purpose of this study. The recommendations are presented in Section 5.4.

### **5.2.4 Summary**

In summary, both secondary research questions have been answered. The image below is a graphical presentation of the summary of the answers to the secondary research questions.



**Figure 5.3 SQ1 and SQ2 summary**

Interesting facts emerged which provided insight into the challenges that companies might face when seeking compliance with POPIA. To answer the main research question, SQ1 and SQ2 had to be answered first. In the next section, the limitations of the study are reviewed.

### **5.3 Limitations of the study**

Uncertainty regarding the date of POPIA's coming into full effect was a problem throughout the research. The researcher is not a legal expert, although legal experts were consulted for guidance. The study did not focus on software development. The study was conducted within a single organisation that needs to comply with specific additional legislation like the FICA Act. Furthermore, the organisation needs to adhere to regulations governed by the specific industry. In the next section, the implementation guidelines are presented.

### **5.4 Research Contributions**

This section will present the theoretical, methodological, and practical contributions of the research.

#### **5.4.1 Theoretical contribution**

This study contributes, both theoretically and empirically, to our understanding of the implementation of POPIA requirements within an SME.

#### **5.4.2 Methodological contribution**

This study demonstrates methodological facets of case study strategy in the field of information security and data protection.

#### **5.4.3 Practical contribution**

This study contributes practically by offering practical recommendations or guidelines that can be utilized by other SMEs in terms of POPI compliance.

### **5.5 Recommendations**

In this section the recommendations are presented to provide a set of implementation guidelines to assist companies in the quest for POPIA compliance. These recommendations are guided by the answers to SQ1 (5.3.1) and SQ2 (5.3.2). These recommendations were derived from further synthesising the themes from Chapter 4. The recommendations are listed below.

- Amend company policy to include POPIA requirements (5.4.1).
- Apply security measures to applications and data (5.4.2).

- Consider migrating to cloud-based services (5.4.3).
- Determine the conflict of requirements between POPIA and other legislation (5.4.4).
- Implement the use of digital signatures (5.4.5).
- Information systems management teams should identify and document security threats (5.4.6).
- Secure information technology hardware infrastructure (5.4.7).
- Staff empowerment should include improvement of cyber security awareness (5.4.8).

### **5.5.1 Amend company policy to include POPIA requirements**

Company policy should be amended and include personal information security. Staff should be made aware of these changes. Some of these policies should be enforced technically and procedurally where possible.

### **5.5.2 Apply security measures to applications and data**

Even though password protection can be considered as an access control measure, coupled with this come additional measures like:

- password management
- access control
- data encryption
- email security

Username and passwords are regarded as the most essential and common forms of security, yet these are the most targeted by hackers. Therefore, additional measures such as minimum password strength, two-factor authentication, and frequent password changes in place greatly enhance the security of a username and a password. Microsoft Windows Active Directory provides password management and allows for the implementation of additional security measures to be applied to passwords. Password hashing should be applied where possible.

Access Control measures should be implemented and documented. This will ensure that the correct users have access to the correct information. This minimises the possibility of information breach. Applications should make use of role-based access that is managed centrally, thereby prohibiting unauthorised access to personal information.

Where possible, personal information should be encrypted. Such information stored in a relational database like SQL Server or MySQL should, where possible and feasible, be encrypted. There are many ways to achieve encryption and these should, at an absolute minimum, render information in an illogical manner, thus making it unreadable in plain sight but perfectly readable after decryption.

Literature indicated that users within an organisation are the most targeted individuals of hackers. Users that receive emails containing harmful files can open these files completely oblivious to the potential risks. Any user can fall victim to this. Therefore, companies should consider the services of companies like Securicom that specialise in ensuring that emails are appropriately scanned for malware content and only after a successful scan are released to users. Businesses that deal with countless emails daily should consider this as an essential form of protection.

### **5.5.3 Consider migrating to cloud-based services**

The number of cyber-attacks has increased (Goel, 2020), and many companies are susceptible to these attacks. Cloud-based services typically implement a standardised security architecture for data and applications, frequently updated to remain current in recognising new and emerging security threats (Kumari & Nath, 2020). The current instability we are facing during COVID-19 has seen an escalation in remote working (Crowley & Doran, 2020). Cloud-based solutions facilitate remote working. Microsoft Azure offers a range of cloud services rendered in accordance with POPIA.

### **5.5.4 Determine the conflict of requirements between POPIA and other legislation**

The heads of companies should ascertain exactly which pre-existing legislative requirements they are bound to and where contradictions in terms of the requirements of POPIA exist. If such contradictions surface, legal advice should be sought immediately to provide clarity.

### **5.5.5 Implement the use of digital signatures**

Digital signatures have been declared a legal form of identification in Canada. Digital signatures incorporate the use of hash functions. These functions are used as a type of cryptography referred to as 'data integrity' (Inam, Kanwal, Zahid, & Abid, 2020). Digital signatures can be considered a reasonable technical measure.

### **5.5.6 Information systems management teams should identify and document security threats**

Where possible, information systems management teams should identify security concerns, document them, and where possible, address these concerns. All new information system projects should include security considerations.

### **5.5.7 Secure information technology hardware infrastructure**

The use of wireless networks is increasingly common and could be considered a communicative necessity within companies. The security of these networks does pose risks, and the following should be considered:

- Firewall installations coupled with the relevant expertise
- Setting up of secure guest networks
- Frequent penetration tests

Firewall installation on its own does not provide absolute protection against digital threats. However, if these devices are set up according to a high standard, they can prove to be very effective in terms of securing networks. Setting up a guest network is essential to protecting the main network from threats while still being able to provide internet connectivity to users other than staff of the organisation that require it. Penetration tests conducted by third parties provide an impartial report of identified threats and allow companies the opportunity to act in a corrective manner. These tests should be conducted frequently as new cyber threats surface regularly.

In addition to the above, security evaluations of other existing infrastructure, like wired networks, should be conducted, documented and where possible, corrected or addressed.

Workstations or computers used by the organisation should adhere to the following:

- Access to removable storage should be limited
- Hard drives should be encrypted
- Reputable anti-virus software should be installed
- Operating systems should be kept up to date

Malware spreads easily through removable devices. Although such access should be limited, this is a step in the right direction and should not be considered an absolute guard against malware.

Windows 10 provides an out-of-the-box solution for hard drive encryption. Most hardware vendors, like HP and Dell, provide this functionality built in. Encryption of hard drives on computers adds another layer of protection in the event of theft or unauthorised access.

Windows 10 was released with an effective anti-virus program and updates for this application are released almost daily. Irrespective of this, reputable anti-virus programs like Sophos or NOD32 should be installed as well. This provides an additional layer of security. Windows 10 releases frequent updates and these include malware protection. Therefore, computers should be updated at least once weekly.

### **5.5.8 Staff empowerment to include improvement of cyber security awareness**

Literature, as well as data, indicated that staff awareness ranging from internal policies to cyber security awareness was very low. Whatever the contributing factors of this phenomenon are, these are critical issues that need to be addressed. Offer informative workshops to increase awareness of cyber security. These workshops should include topics like:

- common hacking techniques and how to protect oneself;
- the importance and meaning of cyber security; and
- the effects and severity of compromised cyber security.

Internal informative workshops relating to policies put in place with the aim of data or information protection. These workshops should seek to:

- enhance awareness levels of internal information protection policy;
- enhance awareness levels of external information protection legislation;
- promote responsible and ethical behaviour in terms of computer use; and
- promote responsible and ethical behaviour in terms of information sharing.



## **5.6 Future research**

Further recommendations for future study are the following:

- This study focused on a specific organisation within a specific sector, and similar studies should be conducted in companies that fall within different sectors.
- The possibility of an independent body that issues POPIA compliance certificates should be researched.

## **5.7 Finally**

Compliance with the POPIA Act is an exercise that should be commenced in companies across the country. This study provides a set of guidelines relevant to parts of the Act that were thematically identified and addressed. These guidelines thus can be used by companies seeking compliance with the Protection of Personal Information Act of South Africa.

POPIA will have an impact on the 2030 UN Sustainable Development Goals. Evidence suggested that the use of accelerators, such as cash transfers, has had a positive impact on South African youth in terms of the development goal aimed at gender equality (Sherr et al., 2020). The information needs of such accelerators, which include the collection and storage of personal information, would fall within the scope of POPIA. Adequate information protection measures should therefore be considered as essential.

In Africa especially, the educational sector is not ready for the 4th industrial revolution (Oke & Fernandes, 2020). POPIA has stringent controls on consent where children are involved (2.1.4). This will impact the storage and collection of student's data.

## REFERENCES

- Abiodun, O., Anderson, D. & Christoffels, A. 2020. Exploring the Influence of Organizational, Environmental, and Technological Factors on Information Security Policies and Compliance at South African Higher Education Institutions, with a Focus on Implications for Biomedical Research.
- Agyei-Bekoe, E. (2013). Empirical Investigation of the Role of Privacy and Data Protection in the Implementation of Electronic Government in Ghana By. De Montfort University.
- Ah Kioon, M.C., Wang, Z.S. & Deb Das, S. 2013. Security analysis of MD5 algorithm in password storage. *Applied Mechanics and Materials*, 347-350:2706-2711.
- Al Farawn, A., Rjeib, H.D., Ali, N.S. & Al-Sadawi, B., 2020. Secured e-payment system based on automated authentication data and iterated salted hash algorithm. *Int J Pow Elec & Dri Syst ISSN, 2088(8694)*, p.8694.
- Aguera, P., Berglund, N., Chinembiri, T., Comninos, A., Gillwald, A., & Govan-Vassen, N. (2020). Paving the way towards digitalising agriculture in South Africa.
- Anthony, R.N. 1965. *Planning and control: a framework for analysis*. Cambridge, MA.
- Babbie, E. & Mouton, J., 2001. The practice of social research: South African edition. *Cape Town: Oxford University Press Southern Africa*.
- Basit, T.N. 2003. Manual or electronic? The role of coding in qualitative data analysis. *Educational Research*, 45(2):143-154. <https://doi.org/10.1080/0013188032000133548>
- Bennett, C.J., Regan, P.M. & Bayley, R.M. 2017. If these Canadians lived in the United States, how would they protect their privacy? *First Monday*, 22(3).
- Boban, M., 2016. Digital single market and EU data protection reform with regard to the processing of personal data as the challenge of the modern world. *Economic and social development: book of proceedings*, p.191.
- Boddy, D., Boonstra, A. & Kennedy, G., 2005. *Managing information systems: an organisational perspective*. Pearson Education.
- Botha, J.G., Eloff, M.M. & Swart, I., 2015, August. The effects of the PoPI Act on small and medium enterprises in South Africa. In *2015 Information Security for South Africa (ISSA)* (pp. 1-8). IEEE.
- Box, D. & Pottas, D. 2014. Improving information security behaviour in the healthcare context. *Procedia Technology*, 9:1093-1103.
- Bracher, P. 2018. Protection of Personal Information Act – Regulations published. <https://www.financialinstitutionslegalsnapshot.com/2018/12/protection-of-personal-information-act-regulations-published/> [27 January 2019].

- Broggt, E., Dokter, E., Antonellis, J. & Buxner, S., 2008. Regulations and ethical considerations for astronomy education research II: Resources and worked examples.
- Burger-Smidt, A. 2016. Appointment of Information Regulator. Werksmans Attorneys. <https://www.werksmans.com/legal-updates-and-opinions/appointment-of-information-regulator-2/> [24 February 2019].
- Buys, M. 2018. Protecting personal information: implications of the Protection of Personal Information (POPI) Act for healthcare professionals. *South African Medical Journal*, 107(11).
- Chaffey, D. & Wood, S. 2005. Knowledge management strategy. *Business information management: improving performance using information systems*.
- Chassang, G., 2017. The impact of the EU general data protection regulation on scientific research. *ecancermedicalscience*, 11.
- Chaum, D., 1992. Achieving electronic privacy. *Scientific american*, 267(2), pp.96-101.
- Cherry, K., 2018. Cross-sectional research method: How does it work. *Advantages and challenges. Student Resources. Available online from: https://www.verywellmind.com/cross-sectional-research-how-does-it-work.* [22 May 2020].
- Childers, J. & Hentzi, G. 1995. *The Columbia dictionary of modern literary and cultural criticism*.
- Collier, D. & Elman, C. 2008. Qualitative and multi-method research: organizations, publication, and reflections on integration.
- Creswell, J.W. 1994. *Research design: qualitative and quantitative approaches*. Thousand Oaks, CA: Sage.
- Creswell, J.W. 1999. *Mixed-method research: introduction and application*.
- Crowley, F. & Doran, J. 2020. Covid-19, occupational social distancing and remote working potential in Ireland (SRERC Working Paper Series, SRERCWP2020-1). <http://hdl.handle.net/10419/218897> [13 July 2020].
- Cyr, D., Head, M., Larios, H. & Pan, B., 2009. Exploring human images in website design: a multi-method approach. *MIS quarterly*, pp.539-566.
- Da Veiga, A., Ophoff, J. (2020). Concern for Information Privacy: A Cross-Nation Study of the United Kingdom and South Africa, 16–29. [https://doi.org/10.1007/978-3-030-57404-8\\_2](https://doi.org/10.1007/978-3-030-57404-8_2)
- Daintith, J. 2009. *A dictionary of physics*. Oxford: Oxford University Press.
- Debruyne, C., Pandit, H.J., Lewis, D. & O’Sullivan, D. 2020. “Just-in-time” generation of datasets by considering structured representations of given consent for GDPR compliance. *Knowledge and Information Systems*.

- Donaldson, S.I. & Grant-Vallone, E.J., 2002. Understanding self-report bias in organizational behavior research. *Journal of business and Psychology*, 17(2), pp.245-260.
- Donalek, J.G. 2005. The interview in qualitative research. *Urological Nursing*, 25(2):124-125.
- Elman, R.J., 1995. Multimethod research: A search for understanding. *Clinical aphasiology*, 23, pp.77-81.
- Facebook. 2018. Facebook's commitment to data protection and privacy in compliance with the GDPR. <https://www.facebook.com/business/news/facebooks-commitment-to-data-protection-and-privacy-in-compliance-with-the-gdpr> [26 March 2019].
- Farquhar, J. & Michels, N., 2016. Triangulation without tears. In *Marketing challenges in a turbulent business environment* (pp. 325-330). Springer, Cham.
- Fenno, R.F. 1986. Observation, context, and sequence in the study of politics. *American Political Science Review*, 80(1):3-15.
- Flick, U., 2004. Triangulation in qualitative research. *A companion to qualitative research*, 3, pp.178-183.
- Flyvbjerg, B. 2006. Five misunderstandings about case-study research. *Qualitative Inquiry*, 12(2):219-245.
- Frank, R. & Wagner, L., 2018. Understanding the Importance of FERPA & Data Protection in Higher Education. An Application: Website at La Salle University.
- Goel, S. 2020. How improved attribution in cyber warfare can help de-escalate cyber arms race. *Connections: The Quarterly Journal*, 19(1):87-95.
- Goldkuhl, G., 2012. Pragmatism vs interpretivism in qualitative information systems research. *European journal of information systems*, 21(2), pp.135-146.
- Goswami, U. 2011. Inductive and deductive reasoning.
- Guba, E.G. & Lincoln, Y.S., 1994. Competing paradigms in qualitative research. *Handbook of qualitative research*, 2(163-194), p.105.
- Guermazi, B. & Satola, D. 2005. Creating the 'right' enabling environment for ICT. In Schware, R. *E-development: from excitement to effectiveness*. Washington, DC: World Bank: 23-46.
- Hallová, M., Polakovič, P., Šilerová, E., & Slováková, I. (2019). Security in SMEs under Enterprise Infrastructure. *Agris On-Line Papers in Economics and Informatics*, XI(1), 27–34. <https://doi.org/10.7160/aol.2019.110103>. Introduction
- Harris, M.A., Levy, A.R. & Teschke, K.E., 2008. Personal privacy and public health. *Canadian Journal of Public Health*, 99(4), pp.293-296.

- Haseeb, M., Hussain, H.I., Ślusarczyk, B. & Jermsittiparsert, K., 2019. Industry 4.0: A solution towards technology challenges of sustainable business performance. *Social Sciences*, 8(5), p.154.
- Henning, M., 2019. *A conceptual approach to increase competitiveness in a typical South African manufacturing SME* (Doctoral dissertation, Stellenbosch: Stellenbosch University).
- Hiller, J., 2016. Epistemological foundations of objectivist and interpretivist research.
- Hoepfl, M.C., 1997. Choosing qualitative research: A primer for technology education researchers. *Volume 9 Issue 1*.
- Houghton, C.E., Casey, D., Shaw, D. & Murphy, K. 2010. Ethical challenges in qualitative research: examples from practice. *Nurse Researcher*, 18(1):15-25.
- Inam, S., Kanwal, S., Zahid, A. & Abid, M. 2020. A novel public key cryptosystem and digital signatures. *European Journal of Engineering Science and Technology*, 3(1):22-30.
- Kandeh, Agbor T., Botha, Reinhardt A., & Futch, Lynn A.. (2018). Enforcement of the Protection of Personal Information (POPI) Act: Perspective of data management professionals. *South African Journal of Information Management*, 20(1), 1-9. <https://dx.doi.org/10.4102/sajim.v20i1.917>
- Kampmark, B. 2015. To find or be forgotten: global tensions on the right to erasure and internet governance. *Journal of Global Faultlines*, 2(2)1-18.
- Kapitzke, C., 2003. (In) formation literacy: a positivist epistemology and a politics of (out) formation. *Educational theory*, 53(1), pp.37-53.
- Koornhof, P. & Pistorius, T., 2018. Convergence between competition and data protection law: a South African perspective. *International Data Privacy Law*, 8(3), pp.277-283.
- Kothari, C.R., 2004. *Research methodology: Methods and techniques*. New Age International.
- Kuhn, T.S., 1962. *The structure of scientific revolutions*: University of Chicago press. *Original edition*.
- Larsen, C. (2019). Data privacy protection in South Africa : an analysis of vicarious liability in light of the protection of personal information act 4 of 2013 (" POPIA ").
- Lincoln, Y. G., & Guba, E. (1985). E. 1985. Naturalistic Inquiry. *London, Sage Publications. Contextualization: Evidence from Distributed Teams." Information Systems Research*, 16(1), 9-27.
- Lincoln, Y.S. & Guba, E.G., 2000. The only generalization is: There is no generalization. *Case study method*, pp.27-44.
- Lincoln, Y.S., Lynham, S.A. & Guba, E.G., 2011. Paradigmatic controversies, contradictions, and emerging confluences, revisited. *The Sage handbook of qualitative research*, 4,

pp.97-128.

- Lu, C.J. & Shulman, S.W. 2008. Rigor and flexibility in computer-based qualitative research: introducing the Coding Analysis Toolkit. *International Journal of Multiple Research Approaches*, 2(1):105-117.
- Lytra, I., Sobernig, S. & Zdun, U., 2012, August. Architectural decision making for service-based platform integration: A qualitative multi-method study. In *2012 Joint Working IEEE/IFIP Conference on Software Architecture and European Conference on Software Architecture* (pp. 111-120). IEEE.
- Mack, N., Woodsong, C., MacQueen, K., Guest, G., & Namey, E. (2005). *Qualitative research methods: A data collector's field guide*. (p1) Research Triangle Park, NC: Family Health International.
- Meijer, P.C., Verloop, N. & Beijaard, D. 2002. Multi-method triangulation in a qualitative study on teachers' practical knowledge: an attempt to increase internal validity. *Quality and Quantity*, 36(2):145-167.
- Nardi, P.M., 2015. *Doing survey research: A Guide to Quantitative Methods (3rd Edition)*. Routledge.
- Noble, C.H. 1999. The eclectic roots of strategy implementation research. *Journal of Business Research*, 45(2):119-134.
- Noble, H. & Smith, J., 2015. Issues of validity and reliability in qualitative research. *Evidence-based nursing*, 18(2), pp.34-35.
- Nouwens, M., Liccardi, I., Veale, M., Karger, D. & Kagal, L., 2020, April. Dark patterns after the GDPR: Scraping consent pop-ups and demonstrating their influence. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (pp. 1-13).
- O'Donnell, B. (2020). Data and Privacy in the Next Decade. *The Technological Revolution in Financial Services: How Banks, FinTechs, and Customers Win Together*, 116.
- O'Leary, Z. (2017). *The Essential Guide to Doing Your Research Project (3rd Edition)*. SAGE Publications Ltd.
- Oberholzer, H.J.G., 2001. *A privacy protection model to support personal privacy in relational databases* (Doctoral dissertation, Faculty of Science, Rand Afrikaans University).
- Oke, A., & Fernandes, F. A. P. (2020). Innovations in teaching and learning: Exploring the perceptions of the education sector on the 4th industrial revolution (4IR). *Journal of Open Innovation: Technology, Market, and Complexity*, 6(2).  
<https://doi.org/10.3390/JOITMC6020031>
- Okumus, F., Bilgihan, A., Ozturk, A.B. & Zhao, X. (Roy). 2017. Identifying and overcoming barriers to deployment of information technology projects in hotels. *Journal of Organizational Change Management*, 30(5):744-766.

- Pearlson, K.E., Saunders, C.S. & Galletta, D.F., 2019. *Managing and using information systems: A strategic approach*. John Wiley & Sons.
- Politou, E., Alepis, E. & Patsakis, C. 2018. Forgetting personal data and revoking consent under the GDPR: challenges and proposed solutions, *Journal of Cybersecurity*, 4(1), p.tyy001.
- Ponterotto, J.G. 2010. Qualitative research in multicultural psychology: philosophical underpinnings, popular approaches, and ethical considerations. *Cultural Diversity and Ethnic Minority Psychology*, 16(4):581-589.
- Robakidze, A. (2019). *Analyzing the Impact of EU General Data Protection Regulation on SMEs*. Seoul National University Graduate School.
- Rubio, N., Chavarria, L. & Mauricio, D. (2020). "Security architecture for the protection of digital assets in SMEs," 2020 International Conference on Electrical, Communication, and Computer Engineering (ICECCE), Istanbul, Turkey, 2020, pp. 1-6, doi: 10.1109/ICECCE49384.2020.9179422.
- Sahay, A. 2016. Peeling Saunders's research onion. Research Gate, Art, pp.1-5.
- Saunders, M., Lewis, P. & Thornhill, A. 2009. *Research methods for business students*. Essex: Pearson Education Ltd.
- Saunders, M., Lewis, P. & Thornhill, A. 2012. *Research Methods for Business Students*. Pearson Education Ltd., Harlow.
- Sherr, L., Cluver, L., Desmond, C., Toska, E., Aber, L., Dhaliwal, M., ... Dugbazah, J. (2020). A new vehicle to accelerate the UN Sustainable Development Goals. *The Lancet Global Health*, 8(5), e637–e638. [https://doi.org/10.1016/S2214-109X\(20\)30103-0](https://doi.org/10.1016/S2214-109X(20)30103-0)
- Shvartzshnaider, Y., Apthorpe, N., Feamster, N., & Nissenbaum, H. (2018). Analyzing Privacy Policies Using Contextual Integrity Annotations. *arXiv preprint arXiv:1809.02236*.
- Smith, D., 2017. Secure pseudonymisation for privacy-preserving probabilistic record linkage. *Journal of Information Security and Applications*, 34, pp.271-279.
- Sophos. 2018. POPI Survey Report – 2018. <https://www.sophos.com/en-us/medialibrary/pdfs/marketing-material/protection-of-personal-information-survey-report-2018.pdf>
- South African Government. (2013). Protection of Personal Information Act, 2013 Ensuring protection of your personal information and effective access to information, (4), 154. <https://doi.org/10.1006/brcg.1998.0994>
- St. Pierre, E.A. & Jackson, A.Y. 2014. Qualitative data analysis after coding. *Qualitative Inquiry*, 20(6):715-719.

- Stalla-Bourdillon, S., Thuermer, G., Walker, J., Carmichael, L., & Simperl, E. (2020). Data protection by design: Building the foundations of trustworthy data sharing. *Data & Policy*, 2, 1–10. <https://doi.org/10.1017/dap.2020.1>
- Staunton, C., Adams, R., Anderson, D., Croxton, T., Kamuya, D., Munene, M., & Swanepoel, C. (2020). Protection of Personal Information Act 2013 and data protection for health research in South Africa. *International Data Privacy Law*, 0(0), 1–20. <https://doi.org/10.1093/idpl/ipz024>
- Swartz, P. & Da Veiga, A. 2016. PoPI Act – Opt-in and opt-out compliance from a data value chain perspective: a South African insurance industry experiment. *2016 Information Security for South Africa – Proceedings of the 2016 ISSA Conference*.
- Trosow, S.E., Tremblay, S. & Weiss, D., 2016. Submission to the office of the privacy commissioner of Canada: Consultation on consent and privacy.
- Turner, D.W. 2010. Qualitative interview design: a practical guide for novice investigators. *The Qualitative Report*, 15(3):754-760.
- Uprichard, E. 2013. Sampling: bridging probability and non-probability designs. *International Journal of Social Research Methodology*, 16(1):1-11.
- Utz, C., Degeling, M., Fahl, S., Schaub, F. & Holz, T. 2019. (Un)informed consent: studying GDPR consent notices in the field. *Proceedings of the ACM Conference on Computer and Communications Security*.
- Van Niekerk, M. (2019). Providing claimants with access to information: A comparative analysis of the POPIA, PAIA and HPCSA guidelines. *South African Journal of Bioethics and Law*, 12(1), 32. <https://doi.org/10.7196/sajbl.2019.v12i1.656>
- Warner, J. 2011. Understanding cyber-crime in Ghana: a view from below. *International Journal of Cyber Criminology*, 5(1):736-749.
- Watanabe, P.J., 2016. An Ocean Apart: The Transatlantic Data Privacy Divide and the Right to Erasure. *S. Cal. L. Rev.*, 90, p.1111.
- Weber, R. 2004. Editor's comments: The rhetoric of positivism versus interpretivism: a personal view. *MIS Quarterly*, 28(1):iii-xii.
- Yin, R.K. 1994. *Case study research: design and methods*. 2<sup>nd</sup> ed. Thousand Oaks, CA: Sage.
- Zimmer, E., Burkert, C., Petersen, T. & Federrath, H. 2020. PEEPLL: Privacy-enhanced event pseudonymisation with limited linkability. SAC '20: Proceedings of the 35th Annual ACM Symposium on Applied Computing, Brno, Czech Republic, 30 March – 3 April 2020. New York, NY: ACM: 1308-1311.
- Žukauskas, P., Vveinhardt, J. & Andriukaitienė, R. 2018. Philosophy and paradigm of scientific research. *Management culture and corporate social responsibility*. London: IntechOpen: 121-140.



Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2020). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. *Journal of Computer Information Systems*, 00(00), 1–16.  
<https://doi.org/10.1080/08874417.2020.1712269>

## LIST OF FIGURES

Figure 3.1 - The research onion .....	20
Figure 3.2 Research design.....	21
Figure 3.3 Inductive research.....	24
Figure 3.4 Interview respondents.....	28
Figure 3.5 Survey respondents.....	32
Figure 3.6 - Research design and methodology summary.....	45
Figure 4.1 Consent .....	49
Figure 4.2 Cross-Legislation impact.....	51
Figure 4.3 Data officer .....	52
Figure 4.4 The company will be able to handle a request for deletion swiftly and accurately	55
Figure 4.5 Deletion of personal information.....	56
Figure 4.6 Industrial regulatory requirements.....	57
Figure 4.7 Always confirms correct client email address .....	59
Figure 4.8 Information management .....	60
Figure 4.9 Information privacy .....	62
Figure 4.10 You are aware of policies within your organisation that provide guidelines for ensuring that emails sent to clients are protected .....	63
Figure 4.11 Policies .....	64

Figure 4.12 You are familiar with the term ‘phishing’ .....	67
Figure 4.13 You use the same password for logging on to your workstation as you use for logging on to social networking sites.....	68
Figure 4.14 One or more of your colleagues know your password to sign into your Windows PC .....	69
Figure 4.15 Reasons for compliance battle.....	70
Figure 4.16 You make use of the USB port on your workstation to charge your cell phone ..	72
Figure 4.17 You make use of USB devices on your workstation to share media (music, images, etc.) .....	73
Figure 4.18 Always locks PC when away from desk .....	75
Figure 4.19 Windows operating system is up to date .....	76
Figure 4.20 You allow others to make use of your PC while logged in with your details .....	76
Figure 4.21 Technical measures .....	77
Figure 4.22 Themes and codes .....	79
Figure 5.1 SQ1 and answers .....	83
Figure 5.2 SQ2 and answers .....	87
Figure 5.3 SQ1 and SQ2 summary .....	91

## LIST OF TABLES

Table 1.1 Research questions and objectives .....	4
Table 2.1 Comparison of different data protection laws.....	18
Table 2.2 Research questions and objectives .....	18
Table 3.1 Philosophy comparison.....	23
Table 3.2 Research methods comparison.....	26
Table 3.3 Interview questions linking themes .....	30
Table 3.4 Likert-scale value and meaning.....	31
Table 3.5 Questionnaire C themes and statements .....	33
Table 3.6 Questionnaire A themes and statements.....	34
Table 3.7 Questionnaire B themes and statements .....	35
Table 3.8 Levels, roles, techniques and research questions.....	38
Table 3.9 Interview respondents with role and appendix.....	39
Table 3.10 Survey colour coding and prefix.....	40
Table 3.11 Unit of analysis, organisational level and roles.....	41
Table 3.12 Lincoln & Guba's (1985) trustworthiness criteria & techniques for establishing them .....	43
Table 4.1 Roles, organisational levels and references.....	47
Table 4.2 Theme and section .....	48

Table 5.1 Research questions and objectives ..... 82

# APPENDICES

## Appendix A – Ethical clearance certificate



P.O. Box 652 • Cape Town 8000 South Africa • Tel: +27 21 469 1012 • Fax +27 21 469 1002  
80 Roeland Street, Vredehoek, Cape Town 8001

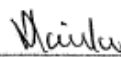
Office of the Research Ethics Committee	Faculty of Informatics and Design
---	-----------------------------------

Ethics approval was granted to MR MARVIN WALTER THEYS, student number 210184043, for research activities related to the MTech: Information Technology at the Faculty of Informatics and Design, Cape Peninsula University of Technology (CPUT).

Title of thesis:	Exploring compliance to the protection of Personal Information Act: Implementation considerations in small software development companies in South Africa
------------------	---

### Comments

Research activities are restricted to those details in the research proposal.

 Signed: Faculty Research Ethics Committee	<u>12/6/2019</u> Date
--	--------------------------



## Appendix B – Interview Protocol

**Interview conducted as part of the study EXPLORING COMPLIANCE TO THE PROTECTION OF PERSONAL INFORMATION ACT: IMPLEMENTATION CONSIDERATIONS IN SMALL SOFTWARE DEVELOPMENT COMPANIES IN SOUTH AFRICA.**

This survey promises the respondent anonymity, confidentiality and the right to refuse at any point. Your signature is required in the space below indicating your acceptance of these conditions and that you have been informed regarding the nature and the purpose of the study.

Name of interviewee: \_\_\_\_\_ Name of interviewee \_\_\_\_\_  
Signature of interviewee: \_\_\_\_\_  
Name of interviewer: \_\_\_\_\_ Marvin Theys \_\_\_\_\_  
Signature of interviewer: \_\_\_\_\_  
Place of interview: \_\_\_\_\_ Cape Town \_\_\_\_\_  
Date of interview: \_\_\_\_\_

**Interview Questions:**

1. POPIA has a requirement that policies should be put in place to protect personal information and I would like to know what your thoughts are on that and if you have implemented or considered the implementation of such policies?
2. Direct Marketing was impacted the most by POPI because of its stringent consent requirement which states that written consent is needed, and I would like to know if you were aware of this and if it would have any impact on the business or its operations?
3. POPIA requires reasonable technical measures be put in place that secure personal information and if you could inform me of some of these measures and possibly its effectiveness?
4. The designation of an information officer is a requirement of POPIA, and its aim is to assist the business with matters relating to POPIA and I would like to know what your thoughts are about this?
5. The request for deletion of personal information is a right granted to individuals by POPI and I would like to know how the business will handle such a request and what are possible issues relating to this that you can foresee?

## Appendix C – Questionnaire C

C

Survey questionnaire instrument conducted as part of the study **EXPLORING COMPLIANCE TO THE PROTECTION OF PERSONAL INFORMATION ACT: IMPLEMENTATION CONSIDERATIONS IN SMALL SOFTWARE DEVELOPMENT COMPANIES IN SOUTH AFRICA.**

This questionnaire promises the respondent anonymity, confidentiality and the right to refuse at any point. Your signature is required in the space below indicating your acceptance of these conditions and that you have been informed regarding the nature and the purpose of the study.

Name of interviewee:			
Designation:	Director <input type="checkbox"/>	General Manager <input type="checkbox"/>	
Place:			
Date:			
Signature:			

Simply check the tick box indicating how strongly you agree with statement.				
<b>Section 1 - Policies</b>				
1. Policies are put in place that ensure data integrity and confidentiality when communicating with clients via e-mail.	Strongly <input type="checkbox"/>	Partially <input type="checkbox"/>	Hardly <input type="checkbox"/>	Disagree <input type="checkbox"/>
In the space below please provide a reason for your selection in statement 1.				
2. Information Security policies are in place to protect client information in general.	Totally <input type="checkbox"/>	Partially <input type="checkbox"/>	Hardly <input type="checkbox"/>	Disagree <input type="checkbox"/>
In the space below please provide a reason for your selection in statement 2.				
<b>Section 2 -Technical Considerations</b>				
3. The company has implemented reasonable technical measures that	Totally <input type="checkbox"/>	Partially <input type="checkbox"/>	Hardly <input type="checkbox"/>	Disagree <input type="checkbox"/>



deal specifically with the protection of personal information.				
In the space below please provide a reason for your selection in statement 3.				
<b>Section 3 - Consent</b>				
4. The company always gets consent from clients to use and store their personal information.	Totally <input type="checkbox"/>	Partially <input type="checkbox"/>	Hardly <input type="checkbox"/>	Disagree <input type="checkbox"/>
In the space below please provide a reason for your selection in statement 4.				
<b>Section 4. Data Officers</b>				
5. The company has started planning for the designation of an Information Officer as required by POPI.	Totally <input type="checkbox"/>	Partially <input type="checkbox"/>	Hardly <input type="checkbox"/>	Disagree <input type="checkbox"/>
In the space below please provide a reason for your selection in statement 5.				
<b>Section 6. Deletion of Information</b>				
6. The company will be able to handle a request for deletion swiftly and accurately.	Totally <input type="checkbox"/>	Partially <input type="checkbox"/>	Hardly <input type="checkbox"/>	Disagree <input type="checkbox"/>
In the space below please provide a reason for your selection in statement 6.				



## Appendix D – Questionnaire A

A

### EXPLORING COMPLIANCE TO THE PROTECTION OF PERSONAL INFORMATION ACT: IMPLEMENTATION CONSIDERATIONS IN SMALL SOFTWARE DEVELOPMENT COMPANIES IN SOUTH AFRICA.

This questionnaire promises the respondent anonymity, confidentiality and the right to refuse at any point. Your signature is required in the space below indicating your acceptance of these conditions and that you have been informed regarding the nature and the purpose of the study.

Name of interviewee:			
Designation:	IT Manager <input type="checkbox"/>	Intermediary Finance Manager <input type="checkbox"/>	Call Centre Manager <input type="checkbox"/>
Place:			
Date:			
Signature:			

Simply check the tick box indicating how strongly you agree with statement.				
Section 1 - Policies				
1. Policies are put in place that ensure data integrity and confidentiality when communicating with clients via e-mail.	Strongly <input type="checkbox"/>	Partially <input type="checkbox"/>	Hardly <input type="checkbox"/>	Disagree <input type="checkbox"/>
In the space below please provide a reason for your selection in statement 1.				
Section 2 - Technical Considerations				
2. Information Security control mechanisms are in place to protect client information.	Totally <input type="checkbox"/>	Partially <input type="checkbox"/>	Hardly <input type="checkbox"/>	Disagree <input type="checkbox"/>
In the space below please provide a reason for your selection in statement 2.				
Section 3 - Deletion of Information				
3. The company will be able to handle a request for deletion swiftly and accurately.	Totally <input type="checkbox"/>	Totally <input type="checkbox"/>	Totally <input type="checkbox"/>	Totally <input type="checkbox"/>
In the space below please provide a reason for your selection in statement 3.				

## Appendix E – Questionnaire B

B

### EXPLORING COMPLIANCE TO THE PROTECTION OF PERSONAL INFORMATION ACT: IMPLEMENTATION CONSIDERATIONS IN SMALL SOFTWARE DEVELOPMENT COMPANIES IN SOUTH AFRICA.

This questionnaire promises the respondent anonymity, confidentiality, and the right to refuse at any point. Your signature is required in the space below indicating your acceptance of these conditions and that you have been informed regarding the nature and the purpose of the study.

Name of interviewee:			
Designation:	IT Support Technician <input type="checkbox"/>	IT Application Support <input type="checkbox"/>	Call Centre Agent <input type="checkbox"/>
Place:			
Date:			
Signature:			



Simply check the tick box indicating how strongly you agree with the statement.				
1. You allow other users to make use of your computer while logged in with your details.	Totally <input type="checkbox"/>	Partially <input type="checkbox"/>	Slightly <input type="checkbox"/>	Disagree <input type="checkbox"/>
In the space below please provide a reason for your selection in statement 1.				
2. You aware of policies within your organisation that provides guidelines for ensuring that emails sent to clients are protected.	Totally <input type="checkbox"/>	Partially <input type="checkbox"/>	Slightly <input type="checkbox"/>	Disagree <input type="checkbox"/>
In the space below please provide a reason for your selection in statement 2.				
3. You always confirm that it is the correct client email that you have on system.	Totally <input type="checkbox"/>	Partially <input type="checkbox"/>	Slightly <input type="checkbox"/>	Disagree <input type="checkbox"/>
In the space below please provide a reason for your selection in statement 3.				

[Empty response box for statement 3]

4. You use the same password for logging on to your workstation as you use for logging on to social networking sites. Totally  Partially  Slightly  Disagree

In the space below please provide a reason for your selection in statement 4.

[Empty response box for statement 4]

5. One or more of your colleagues know your password to sign in to your windows pc. Totally  Partially  Slightly  Disagree

In the space below please provide a reason for your selection in statement 5.

[Empty response box for statement 5]

6. You make use of the USB port on your workstation computer to charge your cell phone. Totally  Partially  Slightly  Disagree

In the space below please provide a reason for your selection in statement 6.

[Empty response box for statement 6]

7. You always lock your PC when you leave your desk. Totally  Partially  Slightly  Disagree

In the space below please provide a reason for your selection in statement 7.

8. You make use of USB devices on your workstation to share media (music, images etc)

Totally

Partially

Slightly

Disagree

In the space below please provide a reason for your selection in statement 8.

9. You are familiar with the term phishing.

Totally

Partially

Slightly

Disagree

In the space below please provide a reason for your selection in statement 9.

10. Your Windows operating system up to date.

Totally

Partially

Slightly

Disagree

In the space below please provide a reason for your selection in statement 10.

## Appendix F – Introductory letter for the collection of research data



### Introductory letter for the collection of research data

**Marvin Walter Theys** is registered for the M Tech (IT) degree at CPUT (210184043). The thesis is titled "**EXPLORING COMPLIANCE TO THE PROTECTION OF PERSONAL INFORMATION ACT: IMPLEMENTATION CONSIDERATIONS IN SMALL SOFTWARE DEVELOPMENT COMPANIES IN SOUTH AFRICA**", and aims to explore and formulate considerations for POPI Act implementation. The supervisor(s) for this research is/are:

Supervisor:

- Prof Ephias Ruhode
- [ruhodee@cput.ac.za](mailto:ruhodee@cput.ac.za)
- 072 802 6329

In order to meet the requirements of the university's Higher Degrees Committee (HDC) the student must get consent to collect data from organisations which they have identified as potential sources of data. In this case the student will use **interviews** and **questionnaires** to gather data.

If you agree to this, you are requested to complete the attached form (an electronic version will be made available to you if you so desire) and print it on your organisation's letterhead.

For further clarification on this matter please contact either the supervisor(s) identified above, or the Faculty Research Ethics Committee secretary (Ms V Naidoo) at 021 469 1012 or [naidoove@cput.ac.za](mailto:naidoove@cput.ac.za).

Yours sincerely

Prof Ephias Ruhode

11 June 2019

**Appendix G – Signed consent in principle form**



I **Kathy Maguire** in my capacity as **General Manager at ManagePlus** give consent in principle to allow **Marvin Walter Theys**, a student at the Cape Peninsula University of Technology, to collect data in this company as part of his/her M Tech (IT) research. The student has explained to me the nature of his/her research and the nature of the data to be collected.

This consent in no way commits any individual staff member to participate in the research, and it is expected that the student will get explicit consent from any participants. I reserve the right to withdraw this permission at some future time.

In addition, the company's name may or may not be used as indicated below. (Tick as appropriate.)

	Thesis	Conference paper	Journal article	Research poster
Yes	✓	✓	✓	✓
No				

Kathy Maguire

11 JUNE 2019

7th Floor, 80 Strand Street, Cape Town 8000  
PO Box 5466, Cape Town 8001

T 021 403 9500  
admin@manageplus.co.za

Manage Plus Fund Administrators (Pty) Ltd. Reg No 1994/00187/07. Director: C Ekerman. An Authorised Financial Services Provider Licence Number 36085

## Appendix H – General manager interview transcript

For the sake of authenticity, the grammatical structure of the sentences has not been changed.

Title of study: **EXPLORING COMPLIANCE TO THE PROTECTION OF PERSONAL INFORMATION ACT: IMPLEMENTATION CONSIDERATIONS IN SMALL SOFTWARE DEVELOPMENT COMPANIES IN SOUTH AFRICA.**

Interview Transcription

Respondent	Margaret Maguire
Respondent Designation	General Manager
Interviewer	Marvin Theys
Date of Interview	25 June 2019

The respondent had a brief introduction outlining the interview.

Marvin: Ok so, interview with Margaret Maguire General Manager at Manage Plus. The interview will be conducted as part of the study EXPLORING COMPLIANCE TO THE PROTECTION OF PERSONAL INFORMATION ACT: IMPLEMENTATION CONSIDERATIONS IN SMALL SOFTWARE DEVELOPMENT COMPANIES IN SOUTH AFRICA. Hi Margaret.

Margaret: Good morning.

Marvin: Margaret, I've got basically just five interview questions and these questions are based off of themes that I've extracted from my literature review and basically all of the other acts that I've explored, ok?

Margaret: Ok.

Marvin: So, it's five questions and the first question will deal with the topic of policies, the second one will deal with consent, the third one with technical measures, the fourth one will be the information officer and then the last one will be the request of deletion of personal information.

Margaret: Ok. Good.

Marvin: Just to give you some background then on the first question, that's based on policies, the GDPR, which is the data protection regulation in the European Union, they leave no room for misinterpretation when it comes to the importance of the adoption of policies, ok? PIPEDA, it is another data protection act that they've got in Canada and they also do not leave any room for misinterpretation. POPI however, only states that you have to take reasonable organisational measures, and by measures it can mean policies, it can even mean the technical measures. So my question basically to you is, I would like to know what are your thoughts on, if you had to implement or to consider the implementation of data privacy policies, what do you think the impact it could have on the business, or just generally what your opinion would be.

Margaret: Generally, in terms of the industry or the country or the way we operate.

Marvin: The way we operate.



Margaret: Ok, it wouldn't have a huge big impact on the way we operate if we had to make things any more stringent because we're not using data to sell to anybody, we're not giving data away. We even very seldom contact our existing client base to up sell them onto other products. So, in the past we used to, but we do not do it anymore, we may now if we've got people on Heritage for example, we may get the agents who are already signed up to work directly with them to phone them to say we now have another product, would you be interested in that, can I come and see you about it. We never ever going to just take our database as it stands, give it to our call centre and say right, fire away and phone everybody and see if they're interested in any other products. We don't do that as it stands. So it's very much a personal relationship between the client and the agent, and the agent would phone back and say, "Look, I've got something else, would you be interested in talking to me about it. So it's not on this mass production basis where we're just saying here's a list, go out there and call them. Has that answered your question?

Marvin: Well, it has actually answered a bit of question 2, but that's fine, it was more like just to implement policies, if you would implement like some kind of a privacy policy within the business like for example, users be sure that whenever you do a customer call to be sure that you do not or ensure that it is the correct person that you are speaking to, maybe even when sending an email out to an client they need to confirm that email address is correct.

Margaret: You see, that is quite difficult. I think our call verification that we do is probably the most fundamental aspect of our policy process because the agent will meet personally with the client, complete the form, bring the form to us. We then have a form which gets captured on to system. before we actually put it live, we will make a verification call. And in that call we verify everything, right down to this is your name, we double check your ID number, your bank details, you did fill in the form, you did meet with that person, you know what the policy is about, you know what you are going to be paying, you know how often you are going to be paying, you know what cover you've got, what it includes, what it excludes, all those types of things. We also now talk about the Medway App which is something new, where they can actually download the Medway App and then they can contact us via that app as well. So we cover that whole range during the verification call. And in doing so I would think, because that's a call recording, you would be saying to the person, "This is you, this is your ID number, this is your phone number, this is your email address.". I'm hoping that that's enough to then say that in future whenever we have any form of communication with that person, we've had the call recording, So, to say that this is your information, so if I'm now emailing you now on that email address that you've confirmed is true and correct, I have to go on the premise that it is in fact you that's reading it. Whether there's someone else sitting on the other end and reading it, I don't know how any company would ever stop that problem from ever happening, you can't. the best we can do is say that you have verified this is your information and we're sending things to you in good faith.

Marvin: Ok. That's a very interesting answer. It seems like there might be even a bigger issue within the entire industry when it comes to authenticating a user.

Margaret: One hundred percent.

Marvin: Thank you for that Margaret.

Margaret: Pleasure.

Marvin: The next question has to do with direct marketing but as you've answered in question one you've already mentioned that Medway itself does not sell any information to anybody else and we don't make outbound calls to attract clients so that's fine.

Margaret: Ok.

Marvin: Question three, POPI requires that reasonable technical measures be put in place to secure personal information and what are your thoughts on that? Or things that you think we could implement, things that are implemented?

Margaret: So, since the implementation of POPI, POPIA, we have been a lot more sort of rigid in our IT processes. So before, you would be aware of this because you helped us institute it, the password login wasn't quite as strictly managed as it is now. It was, you put a password in at the outset and you didn't have to renew your password any given time. Now we've obviously changed that. So first of all there has to be a password for access and secondly those passwords have got to be updated on a regular basis. So, for me that already is protecting each workstation. So from a technical perspective we've got that. We've obviously then got protection on our database, we've got firewalls in place, so we shouldn't have people coming in and being able to steal the data. In essence, and we're very careful about, we haven't even gone the route of putting information on a web portal so that, let's say for example, an agent can log in and go and fetch the information. We haven't even gone as far as to do that yet because we are little bit concerned about security of information. So, the files, you know, sit on our main server, with a firewall, protected access and password control. And for me that's, that seems to be enough at this stage. We would obviously watch to see if any changes are coming through but for now we believe that we got enough cover there. We've had IT people come and do an audit just to see are, do we have enough of a level of protection and our insurers have had to come in and check on that as well because as our insurers, we have a cell within them they have to make sure that we are a hundred percent compliant with all the acts and that was one the things that they did look at. So they're comfortable at this stage and they are also comfortable that we have a backup of data. So that's from a technical perspective. Will you be asking me from a paper perspective? From hard copies?

Marvin: You are more than welcome to.

Margaret: So hard copies pose more of a threat, in my mind. So, we have agents that work all over the country. They go out, they meet with the client. They then get that piece of paper, scanned in to us but they still sit with the original copy. And that for us was a risk. Because agents work for themselves they throw things into the boots of their cars, they drive around, they sometimes driving into areas that are probably a little less safe than we'd like them to be and we've had one or two incidents where the cars had been broken into. The likelihood of people stealing pieces of paper is not that great, but the fact is it can still get out there and those pages contain people's personal identity information. We don't at this point ask for peoples copies of ID's because of the backwards and forwards in over the last couple of years, about "Should you, shouldn't you, do you need it, don't you need it" and we will talk about that a little bit later as well because it is still one of those questions that we're still asking and it comes down to reasonable form of identification. So the "Know your client" aspect but we'll talk about that just now. But those pieces of paper sitting in agents' cars or in their brief cases or on the desk at their house, those are the ones that for me pose a big risk. So we've got a system whereby every month we know which agents have submitted which applications and they have a certain amount of time in which to get those originals to us. Once we

get the original in here we check on system that we've got a perfectly legible copy, we would've done it anyway but we do a double check, and if we're satisfied that we've got a good legible copy as a soft copy, we destroy the hard copy. It gets shredded so that we don't have any pieces of paper that are lying around in anybody's booths or on their desks or anything else, obviously within a reasonable amount of time. If the agents just been to seen a client and they're on their way back and they get hijacked, unfortunately there's not much we can do about that. But we do have other sort of options in place where we're saying let's get that information back from you as quickly as possible.

Marvin: Ok. Alright, and if that type of information is emailed to you, do you guys then discard the emails as well? That would have that as an attachment?

Margaret: Well, yes. We've got a system which cleans up our emails. Nobody is actually keeping all those emails, there is a delete process for that.

Marvin: Fantastic.

Margaret: Ok.

Marvin: Thank you, thanks Margaret. The fourth question is around the designation of an information officer. Now, just to give you some background on this, the appointment of data officers is only required by GDPR and POPI. Now, what a data officer's role is, that an individual within an organisation or a company that is going to, they are going to deal with all issues that relate to privacy violations and informing or up skilling the organisation where they are at regarding the different acts. GDPR in the European Union they actually have got independent bodies that can act as data officers but in South Africa it is recommended that whenever you employ or designate an information officer it must be someone that is in the close vicinity of where the business operates and there was one other article that I read it was recommended that when you employ an information officer, that person should also be aware of other acts that also impact the business and in that way he will be able to then resolve queries at a much higher rate than what you would if the person had no idea of the other acts that also fall within the ambit of the business, so in short basically, an information officer is just to assist the business with matters of the POPI Act, so I would just like to know what are your thoughts on that.

Margaret: So, we, effectively, Craig as the operations director, has always sort of taken on that role. He is the custodian of the data that we have and also being a director of the company and working with, we meet once a month to talk about all the regulatory requirements, any changes in the industry, so if any new act comes into play we would talk about it, we would meet on it, and then we would every month when we meet we would say right, three months ago we implemented the POPIA process into the company, what progress have we made, where are we at with that and we would do that with every other act as well that we're looking at, so it's a forum where we're actually talking about all new legislation's and changes or updated requirements etc. So, the directors of the company are talking about that once a month and in doing so, obviously, Craig's knowledge is quite wide spread, he knows exactly what's happening. We also have to look at our risk management policies where we have to take every act that affects us as a business in the financial services environment and we have to mark it down and at least once a year we have to go back and re-look at that and go, "Right, now lets go through all the acts again and how do those acts impact our business. What is the risk rating.". And we would do that in respect of POPIA as well. So, Craig is very very aware of the information and how it needs to be protected and he is looking at it all the time in respect of all the other acts because he is so well versed on them and he is the custodian at the

moment who would be, if anybody, even if an agent came to us and said, "Please can I a list of all my business for the past five years?", it needs to be an authorised process before he is just given that information. So the agent is obviously welcome to keep copies of or names and addresses and phone numbers of his own client base because they are his clients but when they come to us say, "Please can I have a list of them, my client base?", it tells us first of all that they're not so diligent in doing that, they do rely on us for that information but they need to motivate why they want the list and what they're going to do with it. And ninety percent of the time, unless off course they can give us a proper motivation as to why they would need it, the contact details are removed from those lists. So, even with us having the data, people like our own agents don't even have immediate access to it. Its very very stringent and Craig is monitoring it all the time to see how it fits in with other acts and are we in keeping with the overall regulatory requirements in the country.

Marvin: Ok, alright.

Margaret: Also, I need to just add to that, obviously your knowledge on this and your involvement and the fact that you're now with us, we would obviously have you as the second pinnacle person, who could become our official designated information officer.

Marvin: Ok, alright. Because there's apparently a process involved that information officers have to be registered with the information regulator.

Margaret: Like a compliance officer.

Marvin: And I've contacted the information regulator numerous times and I'm not getting feedback from them, I tried calling them but they've moved offices from Pretoria to Joburg. And I've sent an email to the privacy commissioner in Canada and they responded to me in, I think it was two weeks. And I had a question about their right to deletion, which is the next question, and they weren't too explicit about granting the right for deletion. But then i asked them, look according to it you kind of hint at it and then they responded, they replied to me and said yes, that it is actually the case, that it is covered when you withdraw consent then that is the right to deletion, so.

Margaret: Ok, interesting ways. So that's obviously something in the wheel, they had to come back to us and say, "Now you need to have on official appointed information officer like you do a compliance officer and this is the process.", we would follow the process. So when it comes into being that would be something that would be tabled at the regulatory meeting, it would be put on there until such time as we can actually sign it off to say that that it has been fully implemented, and then we would watch it to see how it's actually working there after.

Marvin: Awesome, awesome. Ok, the last question Margaret. This would be the request for deletion of personal information. Now POPI does grant individuals that right to request that their information be removed from system or hard copy.

Margaret: Ok, so is that, are we talking about a client saying, "I am going to give you this application form, put it onto your system, implement my policy, but then I want my...", because you can't, it's not reasonable to ask that the company then remove your information because you can't administer a policy and talk about, you can't sit and advocate that you know your client if your clients information's been removed. So, at best I would think that what you could do for that client whilst they still have an active policy would be to have their information somehow encrypted so you would keep information up front which would be, give you the bare minimum enough to identify the person

but all the actual information such as their full ID number and address details etc would be encrypted.

Marvin: Okay.

Margaret: We're not at that level yet, but if the act came out and said that this what you need to start doing, we would certainly comply.

Marvin: Well look, there was no specific technical requirements from POPI, for them reasonable, I mean, that is one of the biggest problems with POPI is that it does not give you, for example, the technical requirements, right? It does not even mention encryption at all, whereas GDPR mentions encryption and pseudonymisation, they mention it to say look, you can take these routes, but POPI does not, they say reasonable technical measures which then means I can have a person at a desk with a username and password that can be considered reasonable, for a web portal it can be, it can also just have a username and password, maybe two-factor authentication, that can also be considered reasonable. So, you know the POPI act is not very clear.

Margaret: It is, it's still quite wide open, for a lot of, like you say, interpretation. And when i went to the initial workshops that were held on it the thing that stood out for me was saying that you need to delete people's information after x amount of time etc., etc., and at the time it was contradictory to what the FAIS act stipulates. And we have had it drummed into us from day one that as a financial institution you need to have, follow the FAIS regulations. So, we eat sleep and drink the FAIS regulations. So now, POPIA comes along and says, actually you can't do that with the data, and we going well, do we don't we? Or do we hang on to it five years post termination or do we get rid of it. And now, so that's where we're at as it stands we still abide by FAIS which says you only terminate a person's information five years after the termination of their policy. And that's what we do. So on system, we're busy refining that, but that's ultimately it's gonna work at the click of a button. At the moment it takes a lot more manual intervention to do that. But we are managing it on the basis that everything that's terminated every month, everything that's been terminated for five years gets terminated off system, deleted off system.

Marvin: Or the masking, it's also a technique that gets used. At the company we use a relational database and in order to maintain the relation integrity and all of the transactions that you need to store as a FAIS requirement, it wouldn't be feasible to delete that information, the best we can do is mask that data and have a masked identifier which we can later refer to

Margaret: Hundred percent. So my mind, deleting or masking it's probably the same thing. The average person in the office isn't gonna go and be able to access that person's information after that set amount of time.

Marvin: Look, also, Margaret, the other thing with POPI is that, look, they give the right for a client to request the deletion of information but it will, you are only obliged to delete the information if you no longer require that information to perform a function that you need to in the best interest of the client, for example, having an active policy. You cannot send us a request, look delete my information but you've got an active policy. That's not gonna happen. They must either then terminate or whatever the case my be, but. One thing I have also found in my research is that Google actually had a few legal battles that they lost. They had a person request deletion of information because when he would search for himself on google it would pick up information about him from five years ago. Now, he's a business man he had his own business, and it picked up that he was under sequestration,

now that information can damage his current reputation. he had to fight Google to have it removed but then he won the case. There was however one instance where Google won the case. It was a lady that starred in a short movie and it was posted on YouTube. It had to with Islamic rights and woman abuse. And after the video was posted the poor lady got death threats, and then she contacted Google to have it removed because it's an infringement of her rights but the courts found in favour of google because they did not transgress in anyway.

Margaret: And she had agreed to appear in the movie in the first place. So, I suppose its the same as this where you agree to speak out about something then you know that its for a particular purpose to be viewed by the public fully. So interesting, I could add here that for me, one of the big challenges on the whole POPIA act if I may just give it to you at this stage has been the hard copies of documents. We now since we were made aware of the fact that POPIA was coming into being we started taking steps so we no longer send every single hard copy to metrofile, for example, we don't do that anymore, we destroy the hard copy once we've confirmed we have a soft copy because the FAIS act states that we only need to have a soft copy, we don't need both. our problem lies with the apps that we have had in storage for a number of years and I'm talking pre-two thousand, so those applications are sitting in metrofile in a particular order which depending on the times of the year some of them we're able to identify right down to the box, others not really, it's more about a period that we could track it down to but what we don't have at this stage is a system whereby we can say to metrofile, "Marvin, their policy has been deleted for 5 years now, please go to this box to this file and remove Marvin Theys's file and destroy it". That process we don't know how to do that. We've met with a number of service providers, we've met with metrofile themselves, we've met with other insurers to ask them if they have a system whereby they can do this and nobody can actually tell us how to do this. But I'm sure that you will agree, that it's too expensive for a company, because metrofile is going to ask a fortune, because you're sending them on a wild goose chase into a file, into a warehouse with millions of documents and they must go locate one box, one file and take out one piece of paper and then destroy it, and then send us confirmation to say that that document has been successfully destroyed. Can you imagine the infrastructure and the logistics around trying to manage that process so as much as we are wanting to comply one hundred percent, that is the one area where we have got a little bit more of a struggle so what we're hoping is that the information is sitting in metrofile and metrofile we have spoken to about it they saying to us that there documents are really safe there and no one can get access to those documents. So on that basis we're just hoping that the information could never fall into the wrong hands, there's just too much of it and no one's going to break into a warehouse and look for a particular piece of paper, they not gonna find it, so our hope would be that it would never fall into the wrong hands, at worst it could be a fire, but we're not too concerned with that because we've got soft copies of it anyway, so if you can, in your research come up with a solution to that problem it would help us immensely.

Marvin: Alright Margaret, i think that is it.

Margaret: Pleasure.

Marvin: I just have one last question. Do you perhaps think that you've maybe learnt anything form the interview?

Margaret: I have yes, thank you. It's good to know that where we sit in relation to this kind of act and rest of the world. It's good to know that we're following suite of some of the big powers and I would be very interested to hear you come to me one day to say, "Remember we were talking about how

vague POPIA is? We can now confirm just how specific the act is in Canada and the states, sorry I forget the names, but that we're at that same level, that there's no concern about how they're open to interpretation, that they're actually so fastidious in the policy wording that there's no leave to apply it as you want to.

Marvin: And if you think about it, one of the reasons, I think it is like that is because the application of POPI is very subjective because companies will have different methods and different ways and like you said, this company is also bound by the FAIS act. So, I think that's why, but also its true what you say that it should become a lot more clear.

Margaret: Completely, so we're all trying to comply and do the best we can but we know that there's some loopholes. And even this particular question i posed to you about managing hard copies. Nobody can give me an answer, nobody. So I don't know if while people were sitting here talking about this what they've thought about in terms of historical information. So pre the FAIS act, pre all the other acts, people have got files sitting in warehouses somewhere, and what do you do to fix that.

Marvin: Because we can't erase history.

Margaret: That's exactly it. So we can take on the new acts by all means and we can say that as of today we will not here and now we will definitely not have a file sitting in metrofile that we can't get rid of, but we can't say that for that happened pre 2000 or even early 2000's .

Marvin: I think they will probably make a provision for that.

Margaret: Yes.

The interview closed with me thanking Margaret for her time.

## Appendix I – Administration manager interview transcript

For the sake of authenticity, the grammatical structure of the sentences has not been changed.

Title of study: **EXPLORING COMPLIANCE TO THE PROTECTION OF PERSONAL INFORMATION ACT: IMPLEMENTATION CONSIDERATIONS IN SMALL SOFTWARE DEVELOPMENT COMPANIES IN SOUTH AFRICA.**

Interview Transcription

Interviewee	Elsa Dollman
Interviewee Designation	Admin Manager
Interviewer	Marvin Theys
Date of Interview	04 July 2019

The interviewee had a brief introduction outlining the interview.

Marvin: Alright, welcome Elsa, thank you for agreeing to participate in the study. I would like to inform you that you are free to stop the interview at any time, you do not have to answer if you do not want to answer, if you feel uncomfortable and I have informed you regarding the nature of the study as well and all the information that I get from you it's not going to be, it's going to be anonymized right, because, in a journal article or whatever the case may be I will not refer to you directly.

Elsa: That's fine.

Marvin: So, your identity and your opinion is protected.

Elsa: No worries.

Marvin: So, feel free to be as honest and as open as you can.

Elsa: Okay.

Marvin: So, the first question, I've got five questions for you.

Elsa: Oh, okay.

Marvin: So, just to give you a bit of background, the first question has got to do with POPI's requirement that policies should be put in place to protect personal information, right? Whether it be internal or external policies. Now, I don't know if you are familiar with the GDPR, the General Data Protection Regulation of the EU, it's one of the data protection regulations that had a massive impact on the information technology sector, a lot of companies had to update privacy policies you know, and be more transparent and things like that. So, I would just basically like to know what your thoughts are on that and if you have implemented or considered the implementation of such policies.

Elsa: I think it's a good thing.

Marvin: Okay.



Elsa: If you just look at myself from a personal perspective, I'd want my information protected. I'd not want to be spammed or have unsolicited calls made to me, trying to sell me various products or services unless I've actually intimated something like that. I hate those random calls that, you know, come through. So equally, you know, knowing what I would like I would expect that our clients would expect the same in return. The same protection in respect of their information that they've shared with us knowing that they're safe, knowing that they are not going to be exposed to some form of fraud or have their data exposed to these data companies that solicit information and you don't know, they can't tell you where they've got the information from so, it's not mail listings that we have legally subscribed to where we say we don't mind our information being shared with other service providers like you do get on certain apps on the internet, they ask you that, "Would you like to share the information, could we share the information?". If you're silly enough to say yes and somebody phones you it's a different story but generally you say no because you only want to interact with that particular service provider. So, I think it's a good thing and I think that all companies should implement it, not just for, you know, for their client protection but for own as well. With regards to how far we've implemented it here, we have scripts in our call centre that does allow us to validate that we are speaking to the correct person. We don't disclose information, as a rule, to any party other than the principal insured of the policy and if there is a request by a spouse for some form of information we ask that we receive an email from the principal insured stating that they don't mind that the spouse, or the name of the spouse, ID etc where they live. That person will be phoning and making inquiries on behalf of their claims or their policy and that they give permission etc. We need something in writing just to protect ourselves as well, and that also gets uploaded into the system. A lot of the information that we have is available on our screen because it is captured from an application so, you know, it is important to train staff as well not to disclose just anything either.

Marvin: So, staff training is therefore essential?

Elsa: Absolutely, absolutely. I mean there has been instances where a client has HIV and the partner doesn't know for example, you know, so you can't disclose things, you can't. So, you have to insist on speaking to that person even if it means sending them an email and asking them to contact us at a convenient time. So, so, there is a lot of sensitive information especially in the medical, for medical conditions and so forth that we have to pre-underwrite before we accept an application and we have filters on our systems as well which is available to everybody, all staff members that will indicate that a client has had a particular surgery or has a particular medical condition. That's also available for all to see but it's meant for internal purposes for when we send a claim out to an outside party like Ambledown to say, "Be aware, this person has an underlying diabetic condition", or whatever the case may be because that then sets them off to determine or to decide whether they want to do, to get a doctor's confidentiality report from the client's doctor to see exactly when that condition started and whether the surgery or whatever treatment has been rendered now is not directly related to that because there is a twelve month exclusion so there is a lot of personal information all over on our system with regards to the clients that you can be so careful that you're dealing with the right client, that you're only giving absolutely necessary information to even the insurer, so, you know, as much as you curb things I think staff training and staff awareness is a very big thing.

Marvin: Okay, thank you for your answer. And the second question it relates to direct marketing, which you spoke about in your answer to the first question, and, now POPI has actually made a big impact on the direct marketing sphere in South Africa because it now requires that consent be given in writing to allow direct marketers to contact you. (there were some technical issues) Ok, so like I

was saying, POPI now requires written consent when it comes to direct marketing, so like you said, when you log on to a site and they say we share your information, it's not going to be legally acceptable, you've got to in writing and they've got, they've actually published in the regulations a template of the form that users are supposed to sign. So as you can imagine, this had a big impact on the Direct Marketing business in South Africa and currently there is debate underway between the Information Regulator and Direct Marketing Association of South Africa, so, you know, I don't know what's happening on that side but, in your opinion, in terms of direct marketing, were you aware of this and if it would have any impact on this business or its operations.

Elsa: Well, you've made me aware it now that there is a form that needs to be completed. I don't know necessarily that we're aware of that actual form being utilized here in the business, we usually just put something in writing from the client and confirmation on the telephone that they will be sending something via email. I don't know in the bigger scope of things in that type of marketing environment getting a piece of paper to a person to sign. It's like me going to the police station and asking for, you know, or somebody asking for an affidavit, I can go, do my statement, it gets stamped at the police station, it doesn't mean a word I've said in there is true but it could be used in a court of law. But, ordinarily if you hand that in to any sort of legal concern or you, even us, if we look at an affidavit we think very little of it, unless we're taking that person to court and that court is going to call that person on that document it could all be lies for that matter, so we kind of look for alternative methods of trying to validate information, we would ask a client for example we need a letter from your priest to indicate that you and your ex-wife are living together as husband and wife because we don't cover ex-husbands or ex-wives, we've got to prove that you are living together even though you got divorced, so we'll ask for things from a priest or we will say give us some form of, a bill or something that comes to the residence where that person's name is on the same residence as the principal insured so spouse, ex-wife and ex-husband are living together but they're at the same address that kind of thing. Or a utility bill maybe, the rates bill is still in their name or the one is still dependent on the other one because it's on that person's medical aid card, that type of thing, so just to show the relationship of that, but, just coming back to what you're asking, we don't know of any set form that needs to be filled in, we ask for other documentation because it's the same as if a client says I haven't signed an application form, that's not my signature. For you to go to the client and say give me five signatures, you can sign the same five signatures in one sitting and your signature can be totally different, so we ask for two or three incidences maybe a lease form that you signed 2 months ago and maybe a bank form that you signed a month ago or a, an account you opened up, that form you signed because now you have different time or different time settings and we can then see if the signature is correct or not, because I can easily say that's not my signature, and as I said, sign five signatures looking the same that's different to the one that's on the paper and declare that's not mine. So there's a lot of ways of looking at, when you look at forensics and fraud, there's a lot of ways of looking at actually asking the same question but in a different way so that you, you know, you test it, as I say I'm not aware of any form that, for telemarketing, we don't really do telemarketing here. I do know that on the website you do get the little blocks that you ticked where they ask if they can share your information with other service providers, I was not aware that that is not full proof and that we you needed to have a form filled in. I think sending a form out to clients in this stone age as well with the technology and things that we are, the faxing and the printing and the email and it's just.

Marvin: It just doesn't make sense.

Elsa: It doesn't fit in this century.

Marvin: Yes.

Elsa: It's outdated, it's like snail, what do they call it?

Marvin: Snail mail.

Elsa: The post office. it's just, it's just, I don't know, it, you know, in the cyber science and the things that we have now it, it's ancient, you can't do something like that. Then you could rather, you know, have a, scan your eye or scan your fingerprint or something unique as opposed to getting a piece of paper signed, like I said, an affidavit it actually means nothing. There's so much fraud that can be committed through that piece of paper anyway, it doesn't prove a thing. Well that's my opinion anyway.

Marvin: No, that is, thank you. That's quite powerful. So, onto the next question Elsa, question three POPI requires reasonable technical measures be put in place to ensure that information is protected, right? And, could you maybe inform me of some of these measures and possibly its effectiveness?

Elsa: Technical measures such as in IT controls and things like that?

Marvin: Ja.

Elsa: It's not really my field.

Marvin: No, absolutely.

Elsa: So, I can't talk too much on that. I'm trying to think of examples where.

Marvin: Like maybe users that don't have access to certain folders?

Elsa: Well we do, we do have restrictions on certain things as well, I mean when you're talking about specifically money or commissions and what gets paid out to agents and that kind of thing, there are certain controls where only certain staff are able to view certain information, it's not really applicable to anybody else or to any other staff member. Collections, commission would be, you know, I would think the information is only for a selective few, whoever is working with that. I'm sure there's other information, you can't just go into the report manager for example, our report manager which has got basically interactive user access to pull certain data is limited to certain levels of staff, so different staff on different levels have different access. Obviously, the more responsibility you have and the more access you have to certain things and everything is guarded with passwords and so forth. You also can't share information from those files. If we were to be instructed to send to any particular a second or third party in would have to in an Adobe file or whatever the case may be, not being information that you could just send and quickly altered?

Marvin: Altered yes.

Elsa: You're making me very nervous; I'm looking at you, I know what I want to say but it's not coming out right. So there is limited access to information that you can pull, we also have the company policy, the company handbook, which very specifically states that you cannot divulge any information from the company or any of its clients, you cannot draw information or send that information without having managerial proof or sign off etc, etc. So all of those, there's a lot of things in the handbook that's supposed to be there to protect the company as well that you sign on your employment contract, you sign to say that you've read and understood it and there's an induction program that goes through that entire handbook that covers everything, so you are told, you are laid

the law of what you can or what you can't be talking about in and outside the company and what you can and can't be sharing outside the company, financial information, client information all that kind of things, it's in the handbook and you sign that and that's your agreement that you won't transgress from it.

Marvin: So, like technical measures. I'm not sure but there is a policy that users should always lock their workstations when they leave, right?

Elsa: Well, you know the thing is it does actually lock so quickly after you've got up from your desk, it just locks automatically within 2 minutes its locked and then you need your password to go in. So those basic controls are there.

Marvin: They are there?

Elsa: Yes.

Marvin: Okay, alright. Thank you. The next question relates to the designation of an information officer, right? Every company, according to POPI should have an information officer designated. Now an information officer is basically going to be the individual that deals with the complaints of POPI, that ensures that staff gets kept up to date with what's happening in data regulations, and you know, just basically keeping everyone informed, okay? And I just want to know what it is your, what are your thoughts on that?

Elsa: Well, there are so many changes and things that happen in legislation and it's just changing all the time, it's a living dream thing, that it is good to have an appointed person that is up to date with whatever changes are happening to actually feed that through because you work for the industry, you want to be updated, you want to be empowered with knowing what you can and what you can't and , you know, you want your company to be marked and measured in line with whatever the regulations are and it's a good thing to have someone that regulates that, someone that has good communication skills, and is thorough in making sure that updates are sent out to all the staff, whether its deciding to do a presentation on a , maybe every six months, or whatever, I don't know how frequent the changes are or, you know, just sending brief emails like, "did you know the following?"".

Marvin: Okay, final question Elsa, you can relax now.

Elsa: I'm waiting for the bottom of the tree to fall out.

Marvin: Okay, the last one has to do with deletion of personal information. Now POPI Act grants users the right to request for deletion, okay? And I would like to know how will the business be able to handle such a request, and what do you think are the possible issues that will arise?

Elsa: As much as I agree with POPI, and this is going to sound like a contradiction, I'm very anti-delete. I've had a forensics background and you know, you, a lot of your indicators are from you analysing data, okay, whether that is peoples personal information, if it's based on a geographical area or whatever the case may be, it's based on links and nodes and tying up information to try and determine a way forward if you're looking at fraud and that kind of thing and having an indicator of five clients that maybe came through during the year and there was fraud allegations etc, needing to know that information should they apply again at a later stage because now the insurer has the right to give them thirty days' notice without going into any much detail. Maybe they have a high claiming pattern for example, accidental injuries and that pays a lot of money although it's a stated benefit

now, it pays out a lot of money and now you have these frequent claims coming in and you have these people that have six, seven children whom every other month a child walked into a rusty nail, or burnt with hot water, or the other one was knocked by a car and the other one fell off the bike and everybody's hospitalized and this money is just being paid out, so the insurer has the right then to tell the client we're giving you thirty days' notice because of the high claiming pattern but we suspect there's something going on, there's fraud, but to be able to actually prove it is another thing but the dataset that's there on the claims and so forth tells us what has happened. Now we don't process claims here so the dataset actually sits with Ambledown so that's their problem, okay, they sit with the claims data, but we still sit with the initial claim that we send on, we still sit with the initial documentation about the incident and so forth so if you're just going to have a one liner and you going to say, "Elsa Dolman had five claims and these are the types of claims and this is the amount that's been paid out", its basic information, but you're not flagging Elsa Dolman for having been terminated as a policy because of suspected fraud so when you start deleting data, you can't mine data to actually pick up certain things. So, it's a catch twenty-two situation. It depends on what purposes you're using. Telemarketing, that type of thing, I agree, you just, the information is not for anybody else but when you looking at a business, trying to protect a business, and have certain recourse where you can say to client we're not going to accept your business without being anti-selective, that's the problem. You're sitting with a number of big words here and you're sitting with a scenario that you're wanting to delete information but at the same time you need some form of an indicator, now these nom de plumes, calling people by different names and that, you know, quite frankly when you've got a large book you don't, you're not interested whether it's Mr Smith or Mr Dolman, it's not seen in that personal context, it's seen as the individual that's committed fraud, so you're not really interested in the person's name or ID number as such, you're not interested in sharing their personal detail with anybody else but you need a certain indicator to be able to identify it, you know, to safeguard the business.

Marvin: So, then you would say that it would be in the business's best interest to not grant a request to deletion to anyone because it might impact the way that the business operates.

Elsa: Absolutely. You need to be logical about things. you can't just do because, I don't know.

Marvin: POPI actually does make provision for that.

Elsa: Does it?

Marvin: If a person requests deletion, but you as a business still require that information, then you know, and it's a lawful reason.

Elsa: For your own operational business not necessarily to exploit that person and, you know, maybe have that data go to another company, that company then contacts the client for another product and now you're getting a cutback from that company as well, a commission or something, you're servicing yourself, you're not, it's got to be for moral reasons that you need it, for ethical reasons for running your business not for marketing. I don't know, marketing always has a funny slant in it.

Marvin: So, yes.

Elsa: I think it's really a good and a bad thing, you know.

Marvin: Basically everything, because there's always the pros and the cons and I guess at the end of the day you have to weigh up what works best for the business and I don't think that, okay that's my opinion, but I don't think that a company can ever reach one hundred percent compliance.

Elsa: No, everybody will be a different level.

Marvin: Yes, because POPI impacts different companies differently. So, you can't have a one size fits all. It's not like a car manufacturer, where it states that every car manufactured must have a seatbelt.

Elsa: But there should still be, there should still be consequences to the holding of that information, so that information somehow leaves that company and lands in the wrong hands, you as the company, you're responsible for that information. So, if you decide, and there is a law that says you don't have to delete, you need to be responsible for that dataset.

Marvin: But what are your thoughts on the pseudonymisation, where you use different names to identify client and then you still be able to store that information.

Elsa: I, you know the thing is, you still get a unique, which is probably your ID number, which I can still put in ITC, I can put in a number of any other platforms and still find out who you are, I'm not interested in who you are, I know this sounds terrible, coming from "We must know our clients", you know, FICA, know your client, but what I'm trying to get at is, we're not interested in you, this is going to sound weird, as you or your name, what your name is etc, we just need an identifier that, "Oops, this you", if you know what I'm saying, if you have committed something like fraud or you're a high claimer or something like that, I don't care if your name is Jones or Peter or Smith it doesn't matter to me. Your ID number is that, and your ID number will probably tell me whether you're male or female based on the digits, there's a digit, right I'm looking, if you're over 6 then you're female if you're 5 or under you're male, so I can determine whether you're male or female on your ID, and your age, that's all I can determine on there. What else can I determine, nothing else. If I have platforms like ITC and so forth I can probably go in there and see your accounts and things like that but I mean there again it's responsible use of what's available to the company, you know what I mean, there must be no malice intended, you not going out to witch hunt, you just trying to protect the business. Idea is not to cause unnecessary problems by bad mouthing or blacklisting, you know, that kind of thing. There used to be, in the old days, the used to be the medical aid, used to have forensics forums and you work for different administrators, I worked for Metropolitan, you would have Liberty, you would have Discovery and their forensics staff would come together once month and you would share information on the service providers, mostly doctors, hospitals, pathologists, that type of thing. You'd share the information in terms of the fraud, in terms of the billings, and they would go back, and they would go through the entire dataset, for that particular doctor and they would look for the same anomalies, based on the coding's of different procedures and things, and they would all, everybody simultaneously would act against that doctor, he's got so much money he needs to pay back to the administrators who must pay it back to into the various medical aids, medical aids pay it back to the clients or to the insured pool, depending on where the money was originally paid from. So it's like everything else, it starts up there and it drills deeper, and deeper and the deeper you drill the more the branches, the more it branches out and the more you realize there are twenty other things you should be looking at as well. It's the same with this, you start out with one single question and it branches out into so many different things and then again, like you say, it hits different businesses differently and that then creates its own spiral of another, it's like a family tree.

Marvin: Elsa, are you aware that Canada has two data protection regulations?

Elsa: You did mention it in the last interview, the last err.

Marvin: The questionnaires.

Elsa: Yes, yes.

Marvin: Like one for the private sector and one for the public.

Elsa: Right.

Marvin: So, data protection is something that can become very intricate, but our country has to have some type of legislation in place so that.

Elsa: Are we behind though, are we still third world country when it comes to these types of things or what do you think, we moving on up or?

Marvin: Look, we're not on the level of Canada and the EU when it comes to data protection legislation, but also, I think ours, we, the country should look at the laws of other countries, to help draft our act because in terms of technology South Africa is not far behind.

Elsa: Okay.

Marvin; I mean, a lot of the software development techniques that we use at the company, we are now on par with what's happening in the world, I mean we're not Azure DevOps, we got continuous integration, all those things, so, ja, I mean, no we, South Africa will get there eventually I don't think any time soon, they might.

Elsa: What about penalties for not complying?

Marvin: Well fines can be imposed of up to ten million rands and in some cases, there might even be jail time.

Elsa: is it?

Marvin: Yes.

Elsa: But you don't know of any cases where it's gone to that extreme?

Marvin: No because the POPI act has not come into full effect yet. Only part of the act was made effective so that they could appoint the information regulator, this was done in 2016 and they published the regulations last year. They are currently still at loggerheads with the Direct Marketing Association of South Africa.

Elsa: Which would not surprise me.

Marvin: Just to give you an idea, I contacted the privacy commissioner of Canada and I had a question regarding their data protection legislation, they're out in Canada, they came back to me I think three or four days. I sent an email to South African info regulator and they came back to me after six months just to let me know that they have received my complaint. Elsa thank you very much.

## Appendix J – IT support technician interview transcript

For the sake of authenticity, the grammatical structure of the sentences has not been changed.

Title of study: **EXPLORING COMPLIANCE TO THE PROTECTION OF PERSONAL INFORMATION ACT: IMPLEMENTATION CONSIDERATIONS IN SMALL SOFTWARE DEVELOPMENT COMPANIES IN SOUTH AFRICA.**

Interview Transcription

Interviewee	Reinhard Wolff
Interviewee Designation	Technical Support
Interviewer	Marvin Theys
Date of Interview	26 July 2019

The interviewee had a brief introduction outlining the interview.

Marvin: Ok, so another interview conducted as part of the study and the interviewee is Reinhard Theart. And er the date is the 26th July 2019 erm, Reinhard welcome, thank you.

Reinhard: It's a pleasure

Marvin: for agreeing to take part erm, so i just need to inform you that you've got the right to refuse at any point we can cancel the interview and also any information that you give me, it's going to be treated with confidentiality and erm, I would appreciate it if you could be as open

Reinhard: Ok

Marvin: And as honest as possible and er, yeah if you've got maybe any questions you'd like to ask me?

Reinhard: No, its all good.

Marvin: All good? Ok. So basically, it's going to be five questions er, the theme of the study or the main focus point is the POPI Act, right?

Reinhard: Ok.

Marvin: So er.

Reinhard: To be quite honest I'm not too ...

Marvin: Too familiar?

Reinhard: With the POPI Act.

Marvin: Ok, look the POPI Act is legislation that has been put in place in South Africa which focuses on the protection of personal information.

Reinhard: Data, Ok.



Marvin: Right, so you know globally we've seen a whole lot of emphasis being placed on information privacy, security you know, those type of things. So, I mean South Africa has to follow suit because we need to keep on conducting business with the outside world. Ok, the first question. Er, POPI has a requirement that policies should be put in place in order to protect personal information and i would just like to know what your thoughts are on that and if you have implemented or considered the implementation of such policies?

Reinhard: Yes, ok erm, obviously with user information where you get your accounts and account details and all those private information especially that we got, what we do here, if there's a hacker coming in all those information is out to the world. So first of all we must make sure that our firewall implementation is up to standard so that nobody can come out from the inside. Yes, so and also we do test yearly, an outside company that do penetration tests to see.

Marvin. Alright, if I could just just erm interrupt you quickly. That question specifically has to do with policies itself.

Reinhard: Best Practices, things like your internal network.

Marvin: Yeah, I think more like erm, policies like guidelines that are set in place, like best practices that type of thing.

Reinhard: Best practices. So I mean, we follow best practices of user changing passwords every three months, which comes up that prompts you to change it, that's the one thing that we do. The other thing that we did is also make sure that nobody can put a USB stick into their desktops or laptops to copy or bring other naughty little things onto the network.

Marvin: Ok.

Reinhard: Those are some of the policies or best policies that I have so far implemented here at Medway.

Marvin: Ok. Thank you, thanks for that answer Reinhard, the next question. I don't think really the nature of your role within the business has any bearing to question two but er, it's basically direct marketing was impacted the heaviest by the POPI Act, right? So, I mean, in, you know, erm, the impact, do you think it would have a major impact on the business or its operations? I don't think really it's a question for you so ok.

Reinhard: I don't really deal with marketing.

Marvin: So the we can move on to the next question. So, POPI requires reasonable technical measures to be put in place to protect personal information and could you inform me of some these measure that you've implemented and also possibly its effectiveness and you know, you can even give me, if you think of recommendations even, stuff like you are more than welcome.

Reinhard: Technical measures, technical meaning?

Marvin: Technical measures meaning like you mentioned early if you have firewalls in place.

Reinhard: Ok, so those are the, that side of the scope that we're in now. Like, all our branches have got firewalls ok? Erm, each branch RDP into our network internally. Those what I've done so far on the firewall is to allow only their external public IP's to get into our network so if you're not part of those group you can't get into our network from the outside. Same VPN uses, somebody uses USB

for internet connectivity to connect internally because we don't want to open up infrastructure to the outside world to come and erm, yeah that's firewall. And also, like I said previously, we get a outside company that does penetration tests to see if they can break in and they then give us recommendations on what, if they found a loophole, what to do further to say, "Hey, erm, this we found that this is open, that is open, or the firewall is not up to, the firmware is not up to standard", then we need to make sure that that is rolled out and the necessary security get in place. Also, regarding anti-virus, erm, I implemented Sophos antivirus on all the servers which you cannot uninstall without a proper code so no, even if somebody comes in they can't just go and uninstall Sophos to load ransomware on it, same with those that AV that we implemented erm, it's also protect you against ransomware so they update their services everyday with new viruses, oh new virus erm ransomware protection and also if something comes up onto the server say, ransomware, that antivirus will stop it immediately and revert all the changes that it was made back to the previous one automatically and it will inform you, features so quite but those are only on the servers. Erm desktops we've got. (phone rings and the interview is paused)

(phone call ends and the interview is resumed)

Reinhard: Ok, so all desktops got Nod32 antivirus on.

Marvin: Ok.

Reinhard: Erm, I also, what I've done with those ones, or with those antivirus was to previously before we blocked all USB connections to the machines erm, that would've scanned your USB drive before you will be able to enter it so you can't start that, so that was the previous one, erm, yeah, like I said all desktops, passwords everything and, that's, that's about it. Erm, we don't let any erm, guests connect to our networks because of our security and because of the manner of information that we have -- somebody else where we don't have control over their equipment to connect to our network, so I'm still going to configure the wi-fi so that we can create a guest network but on a separate network, separate IP's, separate subnets, separate gateways, that should give us some erm, what's the word I'm looking for, security that they won't be able to get into our networks, yeah.

Marvin: In terms of emails.

Reinhard: Yes.

Marvin: Are there any?

Reinhard: Yes, all emails are going through Securicom, which gets scanned before it gets delivered to us. They scan all HTML, http websites, all links that are on there. And in fact, I actually stopped it. If a user needs that information they can mail me and say "Please can you release the mail", I will have a look at the mail first to see if there is any security vulnerabilities regarding that and then only release, we don't allow any zip files to come through, that only because some hackers do attempt to put ransomware in zip files and call it photos.zip and a user think hey it's my friend that send it to me and then it opens a whole can of worms. So those are things that we stop. All phishing emails also get stopped but you do get the ones or two's that do get through. I did indicate to people here to, when they find something from someone that they don't know and they're not sure they will always mail and ask first before they will open anything.

Marvin: If emails are configured on their work cell phones?

Reinhard: No, there's no users here except for managers are connected via the phones to emails. All the rest are only purely work desktops.

Marvin: Would you recommend like using erm, you know.

Reinhard: Yes, erm. That one, I would like to implement two factor authentication when you do want to connect to your mailbox on your phone you need to get a pass code from either the firewall or the server to say, "Hey, you are trying to connect now, here is your pass code", whatever number there is you need to put it in before or go through to your login page, so that's the next thing that I might look into.

Marvin: Ok, thank you thank you Reinhard. Erm, ok the next question. I don't really think that question 4 or 5 has bearing on your position, I can tell you. Question 4 relates to the designation of an information officer and that the POPI requires that every company designate an information officer. Now that individual will be responsible for keeping staff informed on the legislation and keeping everybody updated, informing staff, having presentations, showing people what the right and wrongs things are to do, you know, stuff like that and I would like to know what are your thoughts on having something like that.

Reinhard: That's obviously a good thing because not all staff do understand legislation's. You have somebody you need somebody to be able to explain to the everyday person just what it is, this why we do it, so it's a good thing.

Marvin: The last question is the request for deletion of personal information, now this is a right that POPI gives individuals where you can contact a company and ask them to remove your personal information and they have to comply, so what are your thoughts on that and do you think that our business will be able to handle such a request and what are the possible issues relating to this that you can foresee?

Reinhard: Look erm, within our business our data that we keep of our customers are very personal erm, I mean most of those clients that we do have here you need to keep their data until such time that the policy ends and also those information need to be kept for another five years ok, and after that 5 years we can say ok cool, let's clean off the data that we don't need. The reason why we need to keep that is if they go to the ombudsman or there's something related when they had the policies we need to be able to go back and give them info on that specific query that have.

Marvin: Ok. In terms of emails, correspondence that gets sent, attachments that gets added and things like that, do you think it would pose a issue when someone would contact us and say "Look, remove all my information" then we would have to go look at emails and?

Reinhard: That's going to be a bit of an issue because most of our emails get archived for five years as well erm, to go through all of those to delete every single mail from that specific person is gonna take quite a long time to do so yeah that will be a bit of a headache, a lot of work hours to get them totally off your environment.

Marvin: And the information that gets backed up, how far back do we back up?

Reinhard: Ok, we the current backups we've got daily backups that run every day, we've got monthly backups that we keep for a year and then we get yearly backups that we keep for five years. So every fifth year in December we will start with year one again if we get to year five and the same with the monthlies it's been kept for a month and the daily's we keep for two months.

Marvin: Ok. If you were to delete the information from a backup, I mean, would you think that it would be possible?

Reinhard: Look, to go through all the backups so, if we have to delete information from the backups it means that we have to go through each and every backup of the last five years and then the monthlies as well to go and search for that as well to go and search for that because if you take for instance if you have a monthly backup and that guy started in January and in December he decides "Ok, I want all my information removed", we have to go through from December backwards each and every tape to remove all this information off. That's gonna take some time because you gonna have to look for it.

Marvin: Exactly.

Reinhard: So, but if I mean, if you find a first one, because most of your data sits on the same place, it doesn't move around from one place to another

Marvin: Sure sure, it will be easier to look for a record that is stored electronically that what it is to look for a record that is paper based stored at a storage facility.

Reinhard: It will be possible to remove the data but it will take time.

Marvin: Do you have any comments or anything to add to this?

Reinhard: Erm, the next step that I really want to do is to have MAC related authentication so when you connect your machine to the network, if that MAC is not registered to the network then you cannot access the network because currently anyone can plug in a cable and get an IP address. it doesn;t mean they will be able to access all your information because there's authentication in place but that's just an extra layer of security.

Marvin: Ok, we've come to the end of the interview. Reinhard, thank you for participating.

Reinhard: Ok, cheers man.

## Appendix K – Response from the office of the privacy commissioner of Canada

### Response from the Office of the Privacy Commissioner of Canada - INFO-069275

Inquiries Requetes <Inquiries.Requetes@priv.gc.ca>

Mon 2019/03/18 22:03

To: 'marvin.theys@outlook.com' <marvin.theys@outlook.com>

Our file: INFO-069275

Dear Mr. Theys,

This is in response to your enquiry received at the Office of the Privacy Commissioner of Canada regarding withdrawing consent. We apologize for the delayed response.

The mandate of our Office includes oversight of compliance with the [Personal Information Protection and Electronic Documents Act](#) (PIPEDA), Canada's federal private sector privacy law. PIPEDA sets out the ground rules for how private-sector organizations subject to PIPEDA collect, use or disclose personal information in the course of [commercial activity](#).

Generally speaking, where PIPEDA applies, it requires that organizations inform individuals in a meaningful way of the purpose for the collection, use or disclosure of personal information, that they collect, use or disclose personal information for appropriate or reasonable purposes, that collection be limited to what is necessary or reasonable to meet those purposes, and that they obtain the individual's consent before or at the time of collection.

As well, individuals have the right to withdraw consent where appropriate. You may be interested in principle 4.3.8 from [Schedule 1 of PIPEDA](#), which addresses withdrawing of consent:

**4.3.8** An individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. The organization shall inform the individual of the implications of such withdrawal.

PIPEDA also requires organizations to keep personal information only as long as necessary to satisfy the purposes, and destroy, erase or render anonymous information that is no longer required for an identified purpose or a legal requirement.

Our Office has developed guidance and information to help organizations comply with PIPEDA, which may be of interest, including:

- [Guidelines for obtaining meaningful consent](#), which includes a section on withdrawing consent;
- [Form of Consent, an interpretation bulletin on the principle of consent](#);
- [PIPEDA fair information principles](#), including the principles of [consent](#) and [limiting use, disclosure and retention](#);
- [Investigations](#) related to principle 4.3.8 from Schedule 1 of PIPEDA.

We hope this information proves helpful. If you have further questions, do not hesitate to contact our Office at 1-819-994-5444 (outside Canada) or 1-800-282-1376 (inside Canada) and ask for Laurence, an Information Officer familiar with your enquiry. Office hours are Monday to Friday from 8:30 A.M. to 4:30 P.M. (EDT).

Sincerely,

Information Centre  
Office of the Privacy Commissioner of Canada

## Appendix L – Codebook

The codebook presents the code, the description of the code and an example of a quotation.

Code	Description	Example
Archived and backed-up data	Any archiving or backing up of data, specifically challenges.	That's going to be a bit of an issue because most of our emails get archived for five years as well erm, to go through all of those to delete every single mail from that specific person is going to take quite a long time to do so yeah that will be a bit of a headache, a lot of work hours to get them totally off your environment.
Consent	Responses that speak to issues of consent.	We never ever going to just take our database as it stands, give it to our call centre and say right, fire away and phone everybody and see if they're interested in any other products.
Data information privacy	Privacy and the role it plays within the organisation	... even if an agent came to us and said, "Please can I a list of all my business for the past five years?", it needs to be an authorised process before he is just given that information.
Deletion of personal information	Factors that hamper efforts to delete information	It will be possible to remove the data, but it will take time.
FAIS Act	Requirements of FAIS Act that contradicts POPIA	... we still abide by FAIS which says you only terminate a person's information five years after the termination of their policy.
FICA Act	Requirements of FICA that contradicts POPIA	I, you know the thing is, you still get a unique, which is probably your ID number, which I can still put in ITC, I can put in a number of any other platforms and still find out who you are, I'm not interested in who you are, I know this sounds terrible, coming from "We must know our clients", you know, FICA, know your client.
Hard Copies	Challenges faced when dealing with hard copies of information.	So hard copies pose more of a threat, in my mind. So, we have agents that work all over the country. They go out, they meet with the client. They then get that piece of paper, scanned into us but they still sit with the original copy.
Hardware Protection	Factors that enhance the protection of hardware, including networking infrastructure.	... have MAC-related authentication so when you connect your machine to the network, if that MAC is not registered to the network then you cannot access the network because currently anyone can plug in a cable and get an IP address.
Implementation	Implementation of regulatory requirements.	We meet once a month to talk about all the regulatory requirements, any changes in the industry, so if any new Act comes into play we would talk about it, we would meet on it, and then we would every month when we meet we would say right, three months ago we implemented the POPIA process into the company,
Information Officer	Benefits and challenges relating to the designation of an information officer.	That is obviously a good thing because not all staff do understand legislations. You have somebody you need somebody to be able to explain to the everyday person just what it is, this why we do it, so it's a good thing.

Outdated Methods	Challenges working with old technologies or methods	The post office. it's just, it's just, I don't know, it, you know, in the cyber science and the things that we have now it, it's ancient, you can't do something like that.
Policies	Policies within the organisation.	We also have to look at our risk management policies where we have to take every Act that affects us as a business in the financial services environment and we have to mark it down and at least once a year we have to go back and re-look at that and go, "Right, now let's go through all the Acts again and how do those Acts impact our business. What is the risk rating.?" And we would do that in respect of POPIA as well. So, Craig is very aware of the information and how it needs to be.
Software Protection	Factors that enhance the protection of software, including operating systems, email protection, password control, access control and database protection.	I implemented Sophos antivirus on all the servers which you cannot uninstall without a proper code so no.
Staff and Skills Training	Factors relating to staff training and empowerment relating to information security.	it is important to train staff as well not to disclose just anything either.
Vague Requirements	Factors relating the vagueness of POPIA requirements.	the Act is in Canada and the states, sorry I forget the names, but that we're at that same level, that there's no concern about how they're open to interpretation, that they're actually so fastidious in the policy wording that there's no leave to apply it as you want to.
Validation	Procedures in place to validate personal information	We have scripts in our call centre that does allow us to validate that we are speaking to the correct person.
Verification	Procedures in place to verify personal information	We then have a form which gets captured on to system. before we actually put it live, we will make a verification call