

**A Protection of Personal Information Act
Compliance Framework for the City of
Tshwane's Fresh Produce Market.**

by

Pheah Harold Malepeng

**A Protection of Personal Information Act
Compliance Framework for the City of
Tshwane's Fresh Produce Market.**

by

Pheah Harold Malepeng

Treatise

submitted in partial fulfilment
of the requirements
for the degree

MPhil in IT Governance

in the

**Faculty of Engineering, the Built Environment and
Technology**

of the

Nelson Mandela University

Supervisor: Prof. Mariana Gerber

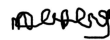
Co-supervisor: Mr Timothy H. Speckman

April 2023

Declaration

I, Pheah Harold Malepeng, hereby declare that:

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



Pheah Harold Malepeng

Abstract

The Protection of Personal Information Act of 2013 (POPIA) is a law drafted to regulate the processing of personal information in South Africa. Its provisions include but are not limited to the usage of personal information for marketing purposes. While it was announced that enforcement of the law would commence in July 2021, many organisations are still in the process of reorganising themselves to comply with this important piece of legislation. Although the Information Regulator's guideline document is available for utilization, organisations are struggling to develop POPIA compliance frameworks tailored to their operational requirements. As stated in section 6.2.1 of the Information Regulator's guideline document, the act calls for the appointment of the an Information Officer by organisations who is required to develop, implement, monitor and maintain a POPIA compliance, framework. With that stated, this study aims to reports about developing a POPIA compliance framework for the City of Tshwane's Fresh Produce Market. The study's primary objective was to develop a POPIA compliance framework for the City of Tshwane's Fresh Produce Market (TFPM) as a collector and processor of personal information. The study had three sub-objectives which were achieved using three research methods, namely literature review, content analysis and semi-structured interviews. Through a literature review, conditions that should be adhered to in relation to collecting and processing personal information were identified. Shifting the focus to the second sub-objective, a vigorous content analysis was performed to investigate the TFPM's current method of collecting and processing personal information. The process involved evaluating the TFPM's SOPs, Service Level Agreement, License Agreement, and the city of Tshwane's Information Communication Technology Framework using the Nexia POPIA checklist. The evaluation results revealed a huge non-compliance gap with regard

to POPIA and personal information conditions. Post development of the POPIA framework the study embarked on an expert review process with the top management of the TFPM to assess their view on the developed POPIA compliance framework.

Acknowledgements

Firstly, I would like to take this opportunity to thank the almighty God for the strength and wisdom he has provided me with to undertake this study under difficult conditions. This was my course after the completion of my first masters degree at another university and it would not have been possible without the support structure that God has offered in the process. Special dedication to my wife Mrs. Mamoroko Nolly Malepeng for her consistent support during my studies and my children Surprise, Mogomotsi, Lethabo and Thato for understanding the reason for my partial absence because of this study. In addition to my support structure, I would like to send special appreciation to my parents who always believed in my abilities from a young age. My late father Mailula Johannes Malepeng who always spoke to me about the importance of education and my mother Molatelo Francinah Malepeng who took it upon herself to become my high school classmate from grade 8 to grade 12 because she had dropped out of school when she became pregnant with me in 1981 and only returned to school when I was doing grade 8 (same school and same class as me). You have been a pillar to me Mom and your presence in all my high school classes made a huge impact in my life.

I would also like to send special appreciation to my late friend Dr. Tebogo Brain Mathabathe who sadly passed away due to COVID -19 complications in January 2021. Dr. Mathabathe was a brother to me and is one person who encouraged me to take this course when I briefed him about my interests in it. How can I forget my late spiritual father Ntate Mosebeletsi Mathabathe whom I lost in July 2021. Ntate Mathabathe played a very important role in my upbringing as a young man as he instilled human morals in my being through his spiritual teachings. **Ke a leboga motswadi wa ka le mo o robetseng teng.** I would also like to thank my study supervisor, Mr.

Timothy Speckman, for being such a wonderful human being. Mr. Speckman made my research treatise journey very easy and enjoyable while instilling discipline. I have learned so much from our engagement sir, thank you for the effort you have made in making sure that this study was completed on time.

Lastly, I would like to thank my manager Mr. Tshifhiwa Madima for his support and encouragement, colleagues, and friends for their unmeasurable support.

Contents

Abstract	ii
Acknowledgements	iv
1 Introduction	1
1.1 Background	1
1.2 Problem Area	4
1.3 Problem Statement	5
1.4 Thesis Statement	5
1.5 Research Objectives	5
1.6 Research Process Workflow	5
1.7 Delineation	6
1.8 Ethical Consideration	7
1.9 Study Contribution	7
1.10 Study Layout	7
2 The Protection of Personal Information	9
2.1 Introduction	9
2.2 Information Technology Governance, Regulations and Legis- lation	9
2.3 Personal Information	10
2.4 Related Personal Protection Regulations	11
2.4.1 General Data Protection Regulation of 2016	11
2.4.2 Promotion of Access to Information Act 2 of 2000	12
2.4.3 Electronic Communications and Transactions Act 25 of 2002	12
2.4.4 Protection of Personal Information Act (POPIA) Overview	13
2.5 The Information Regulator	13

2.6	Information Regulator Guidelines on POPIA Compliance . . .	14
2.7	Benefits of POPIA Compliance	15
2.8	Consequences of POPIA Non-Compliance	15
2.9	POPIA Conditions	16
2.9.1	Accountability (Condition 1)	16
2.9.2	Processing Limitation (Condition 2)	16
2.9.3	Purpose Specification (Condition 3)	17
2.9.4	Further Processing (Condition 4)	17
2.9.5	Information Quality (Condition 5)	17
2.9.6	Openness (Condition 6)	18
2.9.7	Security Safeguards (Condition 7)	18
2.9.8	Data Subject Participation (Condition 8)	19
2.9.9	Conclusion	20
3	TFPM Personal Information Handling Conduct	21
3.1	Introduction	21
3.2	Compliance	22
3.3	The City of Tshwane’s Corporate Governance Structure	22
3.3.1	Governance	23
3.3.2	Management	25
3.3.3	Governance of the TFPM	26
3.4	Content Analysis	27
3.4.1	Preparation Phase	28
3.4.2	Analysis Criteria	28
3.5	Buyer Account Registration Procedure (SOP)	32
3.6	License Agreement (Between TFPM and Fresh-mark Systems)	39
3.6.1	Condition Compliance Test	40
3.7	Service Level Agreement (SLA) (Between TFPM and Fresh- mark Systems)	45
3.7.1	SLA Content Discussion	46
3.7.2	Condition Compliance Test	47
3.8	IT Governance Framework (CoT)	52
3.8.1	Document Discussion	53
3.8.2	Condition Compliance Test	54
3.9	Conclusion	60

4	Research Methodology	62
4.1	Introduction	62
4.2	Research Paradigm	62
4.3	Methodology	63
4.3.1	Analysis Stage	64
4.3.2	Design Stage	64
4.3.3	Evaluate Stage	64
4.3.4	Diffuse Stage	65
4.4	Research Methods	65
4.4.1	Literature Review	65
4.4.2	Content Analysis	66
4.4.3	Expert Review	66
4.5	Conclusion	67
5	Development of a Protection of Personal Information Act Compliance Framework	69
5.1	Introduction	69
5.2	Tshwane Fresh Produce Market Governance Levels	70
5.2.1	Strategic Level	70
5.2.2	Tactical Level	70
5.2.3	Operational Level	70
5.2.4	Office of the Divisional Head	71
5.3	Personal Information Collection	71
5.3.1	Personal Information Collection Workflow and Stake- holders	71
5.4	Personal Information Processing Workflow	74
5.4.1	POPIA Non-Compliance Risk and Impact	76
5.5	Conceptual Framework	77
5.5.1	Accountability	80
5.5.2	Processing Limitations	80
5.5.3	Purpose Specification	81
5.5.4	Further Processing Limitation	81
5.5.5	Information Quality	82
5.5.6	Openness	82
5.5.7	Security Safeguard	83

5.5.8	Data Subject Participation	84
5.5.9	Stakeholder Engagement	85
5.5.10	Conclusion	85
6	Validation of the TFPM POPIA Compliance Framework	86
6.1	Introduction	86
6.2	Expert Interview Process	86
6.3	Findings of the Expert Interviews	87
6.3.1	Section A: Demographic	88
6.4	Section C: Efficacy of the Framework	88
6.5	Section B: Alignment of Practice with the SOPs	90
6.6	Analysis of Open-ended Responses	90
6.6.1	Discussion of Findings	95
6.6.2	Content analysis findings compared to Expert Interview Findings	101
6.7	Conclusion	103
7	Conclusion and Recommendations	105
7.1	Introduction	105
7.2	Research Summary	105
7.2.1	Chapter 1	105
7.2.2	Chapter 2	106
7.2.3	Chapter 3	106
7.2.4	Chapter 4	107
7.2.5	Chapter 5	108
7.2.6	Chapter 6	108
7.3	Review of Study Objectives	109
7.3.1	Sub-Objective 1	109
7.3.2	Sub-Objective 2	110
7.3.3	Sub-Objective 3	111
7.4	Recommendations	111
	References	113

List of Tables

1.1	A Table of the Treatise Layout	8
3.1	POPIA Compliance Checklist (Nexia, 2020)	30
3.2	Summary of Analysed Documentation	32
3.3	Buyers Registration SOP Compliance Test	36
3.4	License Agreement Compliance Test	42
3.5	Service Level Agreement Compliance Test	49
3.6	CoT IT Governance Framework	53
3.7	CoT IT Governance Framework Related Legislation and Reg- ulations	54
3.8	Available IT Governance Measures	56
3.9	CoT ICT Governance Framework Compliance	57
5.1	Types of Personal Information Collected	73
5.2	A Table of POPIA Responsibilities	75
5.3	A Table of Risks from POPIA Non-Compliance	76
5.4	A Table of the Conceptual Framework Processes	78
6.1	Expert Review Respondent Demographics	88
6.2	Framework Efficacy Evaluation Responses	89
6.3	Discussion Question Responses	92
6.4	A Comparison of Content Analysis Findings with the Expert Interview Responses	102

List of Figures

1.1	Research Process Diagram	6
3.1	CoT Corporate Governance Structure	23
3.2	TFPM ICT Governance Structure	27
5.1	Personal Information Collection Workflow	72
5.2	Personal Information Processing Workflow	74
5.3	Conceptual POPIA Compliance Framework	77

Chapter 1

Introduction

In June 2020, sections of the Protection of Personal Information Act (POPIA) 4 of 2013 were signed into proclamation by the president of South Africa. With the remainder of the POPI Act inaugurated on 1st of July 2021, all bodies who collect, process, store and modify personal information in South Africa, are responsible under the POPI Act to comply with the conditions for lawful processing of personal information (Kandeh, Botha, & Futcher, 2018). The primary purpose of this study was to develop a POPIA compliance framework for the City of Tshwane's Fresh Produce Market, in line with the requirements outlined by this legislation. POPIA This chapter presents the background to the study, research context, the problem statement, research objectives and ethical consideration to understand the context of this research treatise (Kandeh et al., 2018).

1.1 Background

Information has become a valuable commodity in contemporary business practices. Therefore, collecting, processing and distribution of it has become the centre of attention for regulators and legislators worldwide. There is global concern about information security data breaches occurring at an alarming rate, with daily incidents reported over the media (Abiodun, Anderson, & Christoffels, 2020). This is of great concern as technology is rapidly moving towards information and datafication being clearly identified, ultimately with the possibility that this information may somehow link to a person in purpose or in effect. This poses as huge identity theft and re-

lated risk should it be obtained (Purtova, 2018). Additional to the risk of identity theft, data breach can harm poses serious threats to organizations, including significant reputational damage and financial losses (Cheng, Liu, & Yao, 2017). One remarkable data breach incident that occurred in the recent years is that of TransUnion where data relating to 5 million consumers and 600,000 organisations were potentially affected by the incident (Beck, 2017). There is global concern about information security data breaches occurring at an alarming rate, with daily incidents reported over the media (Abiodun et al., 2020). This is of great concern as technology is rapidly moving towards information and datafication being clearly identified, ultimately with the possibility that this information may somehow link to a person in purpose or in effect (Purtova, 2018). As such incidents strengthened the need for, the South African regulative house and regulatory bodies to have developed and enacted several pieces of legislation to be on par with their global counterparts (Botha, 2021). The enactment of this legislation is also believed to combat various threats associated with information transaction, in the interest of both individuals and organisations. One such legislation in the context of South Africa is POPIA (Anderson, Abiodun, & Christoffels, 2020). The POPI Act of 2013, is a law drafted to regulate the processing of personal information in South Africa. In its simplest form, POPIA was drafted on the principle that all personal data must be protected by data handlers (Purtova, 2018). Its provisions include but are not limited to the usage of personal information for marketing purposes (Da Veiga, Vorster, Pilkington, & Abdullah, 2017). According to POPIA, personal information is defined by a non-exhaustive list of identifying characteristics that include, but are not limited to, names, sex, age, contact information, medical and financial history, marital status, culture, and language (Botha, 2021). In accordance with POPIA, private and public organisations (including government), are required to comply with the conditions for lawful processing (Kandeh et al., 2018). Kandeh et al. (2018), outline nine steps as a guideline for the implementation of POPIA:

- Step 1: Raise awareness of the POPIA
- Step 2: Change the rules governing data requests to comply with the POPIA

- Step 3: Implement ISO 27001 baseline security controls
- Step 4: Adopt a POPIA compliance culture
- Step 5: Align IT compliance and risk policies and procedures to the POPIA
- Step 6: Take accountability for personal data
- Step 7: Conduct POPIA compliance assessments before procuring software
- Step 8: Build POPIA compliance into the key performance areas and key performance indicators of data management professionals
- Step 9: Finalise requisite policies, processes, and procedures to enable POPIA within the organisation

The City of Tshwane's Fresh Produce Market (TFPM) is a division within the structure of the city's department of Economic Development and Spatial Planning. Its main function is to provide a fresh produce trading platform to its stakeholders in the form of building facilities, Trading Systems, ICT infrastructure, with its secondary function being an ombudsman for producers and buyers regarding the trading conduct of market agencies, thus developing bylaws and ensuring that they adhered to. The primary stakeholders for the market are Market Agencies, Farmers/Producers, Buyers, Freshmark and ABSA bank. Market agencies are the core primary stakeholders of the market as their responsibility entails recruiting farmers from all over the country and selling produce to various buyers on their behalf. Freshmark has been the trading system service provider for over 30 years whilst ABSA bank is the banking partner of the market through which various financial transactions are performed through the Freshmark trading system which is integrated to relevant modules on the ABSA banking system. These financial transactions are performed by market officials in the main, being payments to producers and deposits by buyers.

Before one can become a producer, an agent, or a buyer for the market, they must be registered on the trading system by market officials where in the process, personal information is collected from registrants to ensure a successful registration. This personal information includes identification

number, full names, residential address, and banking account details which are captured electronically on the market's trading system. The market has been collecting this personal information from its stakeholders since its establishment in 1918 and there were no issues because there was no legislation dictating how this information should be collected, stored, processed, and safeguarded. From the 1st July 2021, the market was compelled to collect, store, process and safeguard personal information according to the Protection of Personal Information Act (POPIA), a legislation signed by the South African Parliamentarians in 2019.

1.2 Problem Area

With the TFPM being an organisation that collects, organises, maintains, and uses personal information in its daily operations, it is vital that the organisation complies with POPIA conditions for the lawful processing of information. The consequences for non-compliance to POPIA by specific deadlines can be very severe. It is the prerogative of the information regulator to immediately stop businesses and organisations from processing personal information if found to be in contravention of certain conditions of POPIA by effectively shutting down operations of such businesses or organisations. Further to shutting down operations, the information regulator (given the seriousness of non-compliance) may institute penalty fines of up to R10 million or imprisonment for a maximum period of 10 years (Botha, 2021). However, many organisations in South Africa have been slow to implement POPIA compliance measures according to their business strategies (Ernst and Young, 2020). The concern of implementation challenges is further highlighted by Jafta et al (2020) in their article about an Ontology of South Africa's Protection of Personal Information act, where the authors state that South African government, Civil Society, and businesses are facing both implementation and awareness challenges in their process to comply with POPIA legislation. This in the main is caused by a lack of POPIA compliance frameworks that these sectors use to ensure compliance (Mabunda, 2021).

1.3 Problem Statement

Although the Information Regulator's guideline document on POPIA compliance informs organisations of what must be done to meet POPIA requirements, **organisations are still struggling with how to do it, put them at risk of non-compliance.**

1.4 Thesis Statement

The development of a POPIA compliance framework will assist the City of Tshwane's Fresh Produce Market in complying with the POPIA legislation.

1.5 Research Objectives

The primary objective of this study is to develop a POPIA compliance framework for the Tshwane Fresh Produce Market. Secondary objectives:

- SO1: To identify the requirements for POPIA compliance.
- SO2: To analyse the data handling conduct of the Tshwane Fresh Produce Market in line with POPIA requirements.
- SO3: To address the POPIA conditions by constructing a POPIA compliance framework for the Tshwane Fresh Produce Market.

1.6 Research Process Workflow

The research process diagram labelled Figure 1.1 provides an overview of the process followed throughout this study. A detailed explanation and definitions are provided in Chapter 4 of this treatise. Sub-objectives labelled as SO [number] are shown along with their respective research methods, which when applied lead to the relevant outputs. For example, a literature review was used to identify the eight POPIA conditions that data handling organisations should comply with for lawful processing of personal information, in sub-objective one (SO1). policy documents, service level agreements and standard operating procedures were reviewed in a content analysis (SO2), to analyse the data handling conduct of the TFPM in line with the conditions for

lawful processing. The outputs from SO1 and SO2 were incorporated using modelling and logical argumentation to draft a compliance framework. This output was evaluated by experts during a review process and the feedback was incorporated into the POPIA compliance framework for the TFPM.

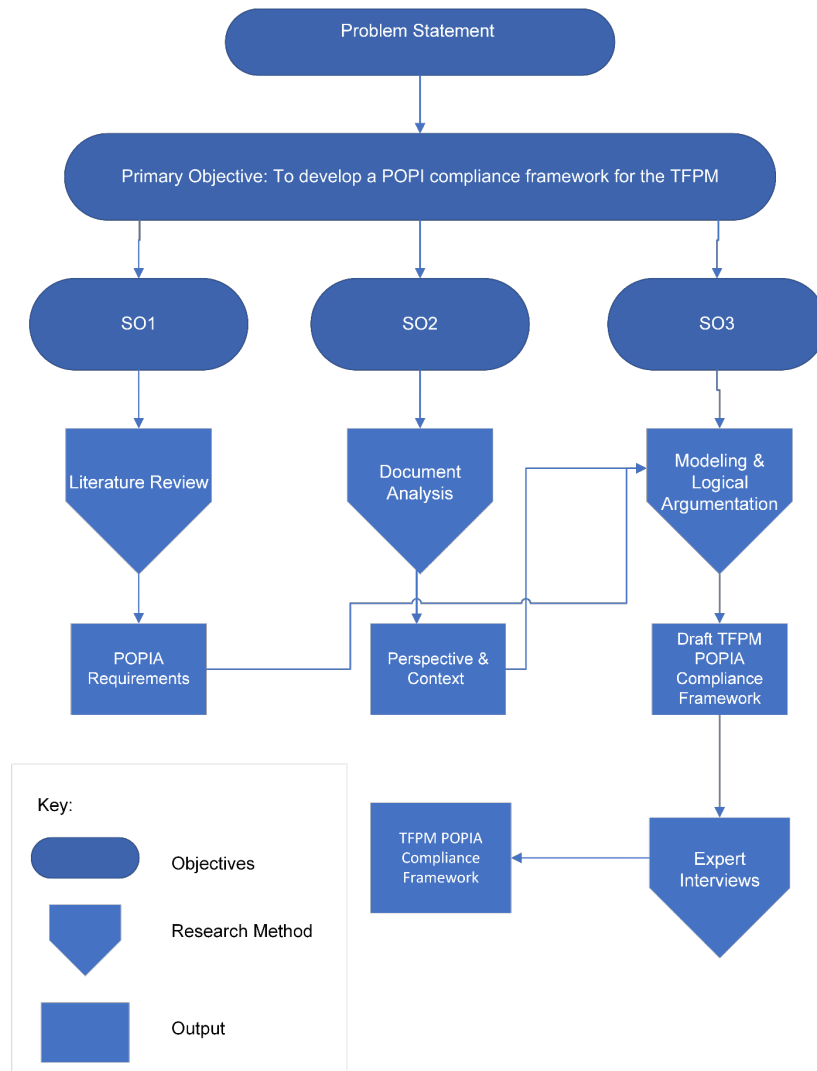


Figure 1.1: Research Process Diagram

1.7 Delineation

The scope of this study was restricted to the City of Tshwane's Fresh Produce Market and does not include other departments within the city. Due to time constraints, effectiveness of the implementation of the framework was not

measured. Existing policy, procedures and frameworks were reviewed to determine the data handling conduct of the organisation.

1.8 Ethical Consideration

Collection of data from study participants only commenced when a participant signed a consent form and approval by the head of the organisation. Collected data was used for the purpose of this study. During the process of data collection, no personal information of a participant was collected. Necessary documentation for the application of ethical clearance was submitted in line with the newly incepted rules about studies involving human participants. Ethical clearance was granted by the Nelson Mandela University Research Ethics Committee (Ref: H22-ENG-ITE-006). To further ensure ethical values in this study, the second principle of the NMU Design Science Methodology Framework was adhered to by ensuring the originality of the compliance framework to be developed.

1.9 Study Contribution

The successful creation of a POPIA compliance framework will have a positive impact in assisting the organisation to comply with different elements of the POPI Act, thus avoiding unnecessary contraventions and litigations. The framework will also add to the body of knowledge in the sense that its usage will not only be limited to Tshwane Fresh Produce Market but other municipalities and organisations dealing with personal information around the province, country and possibly at a global scale.

1.10 Study Layout

The structure of this treatise follows the outline of chapters captured in Table 1.1.

Table 1.1: A Table of the Treatise Layout

Chapter	Title	Brief Description
Chapter 1	Introduction	Introduces the study concepts and the process followed to conduct the study.
Chapter 2	The Protection of Personal Information Act	Identifies POPIA conditions that might impact TFPM as the personal data handler by reviewing literature in this regard. The chapter further analyse the data handling conduct of the Tshwane Fresh Produce Market in line with POPIA conditions for lawful conduct.
Chapter 3	TFPM Personal Information Handling Conduct	Embarks on a process of reviewing relevant documentation to determine the data handling process of the TFPM prior to implementation of the framework.
Chapter 4	Research Methodology	Describes the research methodology that is used in this study in following a systematic a research process.
Chapter 5	Development of a Protection of Personal Information Act Compliance Framework	Development of the proposed POPIA compliance framework developed in line with various governance aspects related to collection, processing and storing of personal information.
Chapter 6	Validation of the TFPM POPIA Compliance Framework	The developed POPIA Compliance framework is being evaluated by expert reviewers in the City of Tshwane's department of economic Development and Spatial Planning.
Chapter 7	Conclusion and Recommendations	The study concluded by summarizing each chapter and the achievement of study objectives is determined. Recommendations are also made based on gaps identified throughout the study.

Chapter 2

The Protection of Personal Information

2.1 Introduction

In Chapter 1, an introduction to the context of this research study was presented. The problem statement and research objectives of the study were defined. Chapter 1 further outlined the research process that was followed as per the NMUDSFM. The primary purpose of this study was outlined as development of a POPIA compliance framework for the City of Tshwane's Fresh Produce Market, in line with the requirements outlined by this legislation. This chapter reviews the relevant literature to identify the POPIA requirements which might impact on the TFPM conduct, as a personal information handler. In this chapter personal information legislation in South Africa are looked at with the inclusion of the General Data Protection Regulation (GDRP) as a closely related legislation applicable in Europe.

2.2 Information Technology Governance, Regulations and Legislation

There is global concern about information security data breaches occurring at an alarming rate, with daily incidents reported over the media (Abiodun et al., 2020). This is of great concern as technology is rapidly moving towards information and datafication being clearly identified, ultimately with

the possibility that this information may somehow link to a person in purpose or in effect. In the contemporary, hyper-connected world of data-driven environments there is a growing need for intensive compliance to protection of information regulations. The principle that all personal data must have protection needs that are supported by data handlers (Purtova, 2018).

As technology has become the primary means for collecting, processing, distribution and storage of information, the protection of this information therefore has been deemed the responsibility of information technology governance (ITG). ITG is defined by Raodeo (2012) , as the decision-making process about information technology (IT). The author further expands this definition by stating that good ITG ensures optimization of IT assets, alignment to the business strategy, value for the organisation and good management of risk. There are several ITG frameworks that have been developed to ensure realization of the organisational objectives. Information Technology Infrastructure Library (ITIL), Control Objectives for Information Technology (COBIT), ISO/IEC38500 are the popular IT governance frameworks adopted by majority of companies and organisations globally including South Africa to define generally accepted rules, processes, and characteristics in alignment with the business objectives (Goeken & Alter, 2008).

Attached to the aspects of ITG are regulatory and regulative frameworks. These frameworks are enforceable by governments around the world to standardize the conduct of organisations with regard to IT, thus ensuring that IT related risks are controlled in the best interest of the citizens (ChePa, Bokolo, Rozi, Nor Haizan, & Masrah, 2015). The regulative and regulatory aspects of ITG are not adopted by companies and organisations to increase their profitability or productivity, but rather to ensure compliance with statutory requirements which seek to protect citizens against vulnerabilities associated with IT systems (Marx, Moolman, & Ngwenya, 2016).

2.3 Personal Information

According to POPIA, personal information is defined by a non-exhaustive list of identifying characteristics that include, but are not limited to, medical and financial history, marital status, culture, and language (Botha, 2021). Botha (2021), further expands on personal information which POPIA pro-

vides on processing prohibiting its use by the health care sector by health care practitioners unless there is consent from the data subject as per the list below:

- Personal information on religion
- Personal Information on Philosophical beliefs
- Personal Information on Race or Ethnic Origin
- Personal Information on Trade Union Membership
- Personal Information on Political Persuasion
- Personal Information on Health
- Personal Information of Sex life
- Personal Information on Biometric
- Personal Information on criminal behaviour

Personal information generally defines the identity of a person as reflected in the literature. Discussions about extending the scope of personal information have been on the rise in recent years, in the data protection community (Purtova, 2018). Notably, according to research conducted by Price Water Coopers, many consumers are becoming increasingly concerned about how their personal information is being handled and shared with third parties (Da Veiga et al., 2017).

2.4 Related Personal Protection Regulations

This section gives a summarised overview of related data protection regulative acts followed by an overview of the POPI Act in Section 2.5.

2.4.1 General Data Protection Regulation of 2016

Because of the significant amount of personal information flowing internationally, data protection it is important for the European Union (EU) and the United States of America (USA) regarding laws around data privacy.

It is estimated that the two economies generate an estimate of \$260 billion on annual digital services trade and this trade relationship involves personal information (Schwartz & Peifer, 2017). It is generally believed that the state of privacy protection laws of the EU is more comprehensive than that of the US (Hiller, McMullen, Chumney, & Baumer, 2011). The General Data Protection Regulation (GDPR) is a regulation of the European Parliament and Council, enacted in April of 2016. This regulation defines a uniform data security law on all European Union (EU) members. The purpose of the GDPR is to protect the rights of natural persons where personal data is handled in EU member states. Article 8 of the EU Charter of Fundamental Rights. Everyone has the right to the protection of personal data concerning him or her is the subject of the GDPR. Like the POPI Act, the GDPR defines specific conditions for personal data handling and specific instances for exemption (Parliament & Council of the European Union, 2016).

2.4.2 Promotion of Access to Information Act 2 of 2000

The Promotion of Access to Information Act (PAIA) 2 of 2000 is a regulative act drafted to fulfil Section 32 of the SA Constitution. According to Section 32, of the Constitution, state and private organisations are obliged to act in an accountable and transparent manner by providing access to information. Furthermore, this act also details the grounds under which a public or private organisation could refuse access to information. It should be noted that before the amendment by POPIA of 2013, PAIA pertained to transparency (or the lack thereof) of information held by public and private organisations and not necessarily personal information (DST SA, 2016). Since the amendment of PAIA through the POPIA, compliance to both POPIA and PAIA will be monitored by the Information Regulator, an independent body set up to monitor complaints relating to these acts (DST SA, 2016).

2.4.3 Electronic Communications and Transactions Act 25 of 2002

The ECT act is law No.25 that was promulgated by the South African parliament in August of 2002 with the purpose of facilitating and regulating

electronic communications and transactions and for provision of development of the national e-strategy in South Africa. The law was further developed to promote access to electronic communications and transactions by Small, Medium and Micro Enterprises (SMMEs) and to encourage the utilization of the e-government services. Chapter 8 of this legislation defines the scope of personal information and the principle of electronically collected personal information. The ECT act does not only cover the e-commerce type of transaction, but it also aims to deal with privacy issues, domain names and cyber-crime (Eiselen, 2014). Although the ECT Act, alludes to the need for protection of privacy in the context of consumer rights and that of information security, when transacting electronically, the act does not cover the aspects of the POPI Act extensively (Kandeh et al., 2018).

2.4.4 Protection of Personal Information Act (POPIA) Overview

POPI The Protection of Personal Information Act of 2013 (POPIA) is a regulative act drafted to regulate the processing of personal information in South Africa. Its provisions include but are not limited to the usage of personal information for marketing purposes. While it was announced that enforcement of the act would commence in July 2021, it is reported that many organisations continually grapple with reorganising themselves to comply with this important piece of legislation (Da Veiga et al., 2017).

2.5 The Information Regulator

The Information Regulator (IR) is the statutory body that regulates handling of information, with its primary mandate being protecting personal information, promoting access to information and monitoring and enforcement of POPIA as outlined by Adams and Adeleke (2020) . It is a requirement within the scope of POPIA that certain categories of personal information be authorised by the IR before the responsible parties may commence in processing them. Such categories of personal information would require prior authorization once and not every time such personal information is processed as outlined in section 57 of POPIA (Milo & Dela, 2021). The first category of

such personal information that the IR provides guidelines on involves unique identifiers of data subjects for the purpose other than the initial one that it was intended to collect, with examples being the bank account numbers, identity numbers and telephone numbers. The second category involves personal information on criminal behaviours or any objectionable conduct on behalf of the third parties. The third category involves personal information that is to be processed for credit reporting while the final category focuses on processing of special personal information and personal information on children exchanged with third parties in countries where the level of protection is not regarded as adequate for the processing of personal information (Milo & Dela, 2021). Milo (2021), further advises that it is important for responsible parties to take note of the prior authorization requirements and various deadlines outlined by the IR as hefty fines and penalties can be actioned against them.

2.6 Information Regulator Guidelines on POPIA Compliance

To aid in compliance with POPIA, the Information Regulator issued guidelines on developing codes of conduct and checklists, the initial step of complying to POPIA. These codes of conduct are a set of rules applicable to certain information, activities, bodies, professions, and industries regarding POPIA conditions. Embedded in the guidelines are also appointment, registration and responsibilities of the information officer who is part of the POPIA compliance requirements (Greal, Mngomezulu, Tembedza, & Blom, 2021).

The section of POPIA which sets out the responsibilities of the information officer came into effect from the 1st of May 2021. According to this section of the act, the information officer must be registered with the Information Regulator before commencement with their responsibilities. Although all POPIA conditions are enforceable by law, the act includes provisions for the Information Regulator to exempt organisations on certain conditions in certain circumstances (Greal et al., 2021).

For example, it is permissible within the prescripts of POPIA that the

information regulator may provide exemptions to personal information processors to breach one of the conditions for lawful processing within POPIA provided that the public interest outweighs the interference to privacy of the data subject or there are clear benefits to the data subject or third party (Greal et al., 2021). There are no businesses or organisations in South Africa that do not know by now that they need to be compliant with POPIA. The challenging part is that most businesses see this compliance as a grudge purchase instead of an opportunity. For them it is about ticking the compliance box (Job, 2021). Job (2021) further advises that businesses and organisations should move away from treating POPIA compliance as a regulation checkbox exercise but rather regard it as an opportunity to build resilience.

2.7 Benefits of POPIA Compliance

During the cyber security and resilience strategy presentation conducted by Skinner (2021), he argues that businesses and organisations should regard POPIA as a revenue generation vehicle as opposed to an additional cost or a burden to business. The presenter further highlights that business opportunities can be created through compliance with POPIA as one cannot be resilient unless they are compliant (Job, 2021). To better capitalize on POPIA while complying, businesses and organisations need to know and understand their customer base, understand what data they possess about them and have knowledge of where this data resides, thus in that way they will be able to maximize the benefit of data in their possession (Job, 2021). Although personal data has a potential of maximizing business and organisation benefits, the presenter further advises that these businesses and organisations need to be in a position where they will be able to remove personal data from their database if asked to by their customers so as to avoid contravention of the act.

2.8 Consequences of POPIA Non-Compliance

The consequences for non-compliance with POPIA by the stipulated deadline can be very severe. It is the prerogative of the Information Regulator

to immediately stop businesses and organisations from processing personal information if found to be in contravention of certain conditions of POPIA by effectively shutting down operations of such businesses or organisations. Further to shutting down operations, the information regulator, given the seriousness of non-compliance, may trigger penalty fines of up to R10 million or imprisonment for a maximum period of 10 years. Thus, it is in the interest of organisations to comply with the conditions of POPIA (Botha, 2021).

2.9 POPIA Conditions

Although this legislation consists of 11 chapters only a few important aspects from various chapters are highlighted in this study. This study's primary focus is on Chapter 3: Part A of the Protection of Personal Information Act (POPIA) No. 4 of 2013 which sets out eight conditions for lawful processing of personal information by personal information handling organisations. Although the study does not include the exploration of elements outlined in Part B of the same chapter, it entails setting out conditions for prohibiting the processing of special personal information which is also important to be noted by personal information handlers. The primary conditions that the study focuses on are as outlined below:

2.9.1 Accountability (Condition 1)

This condition is displayed in section 8 of the POPI act, and it highlights that it is the responsibility of the data processor to ensure that lawful processing of personal information is always adhered to for the determination of purpose, means of processing and the processing itself (The Presidency, 2013, p. 23).

2.9.2 Processing Limitation (Condition 2)

Section 9 of the POPI act outlines the processing limitation condition, which ensures that processing of personal information is handled in a lawful manner that does not infringe on privacy of the data owners. Embedded in this condition are sections 10, 11 and 12 which outline that personal information can only be processed if the purpose of processing is displayed, is adequate, relevant, and non-excessive. The condition further highlights under section

11 that processing of personal information should be consented to by the data subject, there must be justification for processing and the data subject must be allowed to object. The conditions further state that personal information must be collected directly from the data subject except under the circumstances outlined under subsection 12. (The Presidency, 2013, p. 24).

2.9.3 Purpose Specification (Condition 3)

This condition is outlined by section 13 of the POPI act that the collection of personal information should be done for a specific, explicit, and lawful purpose aligned to the functions of the collecting party. The section further emphasizes that this collection must be done with the personal information owner being aware of the purpose (The Presidency, 2013, p. 25). In section 14 of the purpose specification condition, the law further outlines the retention and restriction of personal information record conditions. This section states that the personal information records must not be retained for longer than necessary for achieving the intended purpose that the information was collected for unless under circumstances mentioned under subsections 2-8 of the purpose specification condition (The Presidency, 2013, p. 25).

2.9.4 Further Processing (Condition 4)

This condition entails section 15 of the POPI act. The section states that further processing of personal information must be done compatibly and according to the original purpose of collection by the responsible party in line with section 13. To assess the compatibility and in accordance with further processing for personal information collection, subsection 2 and 3 of this section of the law outlines lawful conditions that must be taken into cognizance (The Presidency, 2013, p. 26).

2.9.5 Information Quality (Condition 5)

This condition makes up section 16 of the POPI act and it states that reasonable and practical steps must be taken by the personal information processor to ensure accurate, complete, not misleading, and that personal information must be updated where necessary. The section further states that in ensuring personal information quality, the responsible party must have regard

for the original purpose of collection of personal information and its further processing (The Presidency, 2013, p. 28).

2.9.6 Openness (Condition 6)

This condition is made up of section 17 about the handling of documents and section 18 about notifying the data subject when collecting personal information. Section 17 states that documentation of all processing operations must be maintained by the responsible party as referred to in section 14 of the act while section 18 states that the responsible party must ensure that the data subject is made aware of conditions outlined in subsection 1-3 of section 18 of this condition (The Presidency, 2013, p. 30).

2.9.7 Security Safeguards (Condition 7)

This condition substantiates section 19 of the POPI act about the security measures on integrity and confidentiality of personal information. The section outlines conditions that the responsible party must adhere to, to ensure integrity and confidentiality of personal information in their possession or under their control for the prevention of the following possible threats (The Presidency, 2013, p. 32):

- Loss of personal information
- Damage to personal information
- Unauthorised access to personal information
- Destruction of personal information
- Unlawful access or processing of personal information

Section 19 subsection 2 under this condition further displays the following measures that must be put in-place to prevent threats outlined by subsection 1:

- Identify all reasonably foreseeable external and internal risks associated with personal information in their possession.
- Establish and maintain appropriate safeguards against identified risks.

- Regular verification of the effectiveness to safeguard measures in-place.
- Continual improvement of safeguarding measures in response to new risks and ineffectiveness of the previous measures.

Section 20 under condition 7 displays further conditions that must be taken in consideration on information processed by operators or persons acting under authority. The section mentions that such processors must only process personal information with the knowledge of the responsible party, or the responsible party must have authorised the processing. The section further requires that this personal information be treated with a high level of confidentiality and must not be disclosed. Section 21 under the same condition, mentions security measures regarding personal information processed by operators. The section outlines the need for a written contractual agreement between the responsible party and the operator in ensuring the establishment and maintenance of security measures on personal information that is under their control. This section further states that it is the responsibility of the operator to immediately inform the responsible party whenever there are reasonable grounds that personal information has been accessed or acquired by an unauthorised person. This condition further displays the required steps to follow about the notification on security compromises under section 22, subsection 1-6 (The Presidency, 2013, p. 32).

2.9.8 Data Subject Participation (Condition 8)

Section 23 of the POPI act describes conditions that personal information must be accessed by the data subject. These conditions are outlined in detail in subsection 1-5 of section 23 of the POPI act under condition 8. Further to accessing their personal information, a data subject has it under the prescripts of POPIA law to request correction or deletion of their personal information in the control of the responsible party. Section 24, subsection 1-4 outlines in detail the circumstances that the correction and deletion may be undertaken while section 25 defines through section 53 of the promotion of access to information act (PAIA), the way personal information must be accessed for correction or deletion as outlined in section 23 of the POPI Act (The Presidency, 2013, p. 36).

2.9.9 Conclusion

This chapter gave an overview of the POPIA. The chapter began by defining ITG and the role of regulations and legislation within the ITG sphere. Personal information was also defined in this chapter as information that could lead to the identification of an individual. To protect the individuals that this information identifies, several information disclosure and protection regulations were briefly summarised, namely, the GDPR, PAIA and the ECTA. In line with the objective of this chapter, an overview POPI Act was given. This entailed discussing the role of the Information Regulator, the benefits of POPIA compliance, the consequences of non-compliance and finally, the eight conditions for lawful personal information handling according to POPIA. It was periodically encountered in literature that organisations continually grappled with POPIA compliance. As discovered in Section 1.3 of this treatise, this is often attributable to the lack of a common POPIA compliance framework. Chapter 3 presents the findings of a review into the personal information conduct of the TFPM, which was conducted by means of a content analysis.

Chapter 3

TFPM Personal Information Handling Conduct

3.1 Introduction

In Chapter 2, the eight conditions of POPIA, for the lawful processing of personal information were discussed. It was also established that the conduct of organisations is controlled through governance processes. These processes entail the writing and dissemination of various policies, procedures and agreements that dictate the conduct of operations within the organisation. Although there were no documents that directly aim to enforce POPIA compliance with TFPM and CoT, policies and procedures were analysed to check elements that might have addressed the POPIA requirements. In this chapter the City of Tshwane's corporate governance framework and the standard operating procedures (SOPs) of the TFPM are explored and analysed in line with the POPIA conditions using content analysis process. Content analysis can be seen as an unobtrusive research approach in that it can be used to analyse naturally-occurring data. The processes include constructing a theoretically valid research question or hypothesis; identifying and sampling content; developing systematic coding schemes which are implemented; testing for interrater reliability; and performing analysis (Huxley, 2020). The outcome of this process assisted the researcher in determining the data handling conduct (compliance) of the TFPM with regard to the POPIA conditions.

3.2 Compliance

Kharbili, Stein, Markovic and Pulvermiller (2008) emphasize the importance of ensuring compliance with processes, legal regulations, governance guidelines, and strategic business requirements as an essential condition for good control of business behaviour. The authors further state that the implementation of compliance requires measures for modelling and enforcing. Similarly, Brotby (2009, p. 5), proposes that conducting business in a manner that conforms to the rules of society embodied in law and ethical customs is good governance. Furthermore, senior management is seen to be responsible and legally liable for failing the requirements of due care and due diligence where such good governance practices are not followed. It is believed that incidents such as the Watergate Scandal and the Enron Scandal, among others, were the basis for modern governance requirements. Investigators at the time highlighted organisational control failures and a lack of requirements for organisations to report on internal controls, as the centre of the scandal (Brotby, 2009, p .5).

3.3 The City of Tshwane's Corporate Governance Structure

Claessens and Yurtoglu (2012) describe corporate governance as a normative framework that sets the rules under which organisations should operate. Such rules are informed by sources such as the legal system, the judicial system, financial markets, and labour markets. Figure 3.1 depicts the corporate governance structure of the City of Tshwane (CoT). The structure is divided into parts as guided by the Control Objectives for Information and Related Technologies (COBIT) 5 IT Governance framework. COBIT was initially developed to support (financial) audit professionals who were increasingly confronted with automated environments. ISACA released the first edition of COBIT in 1996 as a framework for executing IT audit assignments. This first edition was quickly succeeded by the second edition in 1998, which was built around a comprehensive set of control objectives for IT processes (De Haes, Van Grembergen, Joshi, & Huygh, 2020). De Haes and Van Grembergen (2004) provide a clear differentiation between ITG and IT management.

The authors define IT governance as the organisation s Board, executives management and IT management having a capacity to exercise control of the formulation and implementation of IT strategy in ensuring the fusion of business and IT, while IT management is focused on the effective supply of IT services and products and the management of IT operations. The first part of the structure outlines the governance aspects of the CoT’s ICT, while the second part, being management, displays the operational aspect of the CoTs ICT. The governance phase of the CoT framework consists of three tiers of committees, while the management phase consists of just one operational committee.

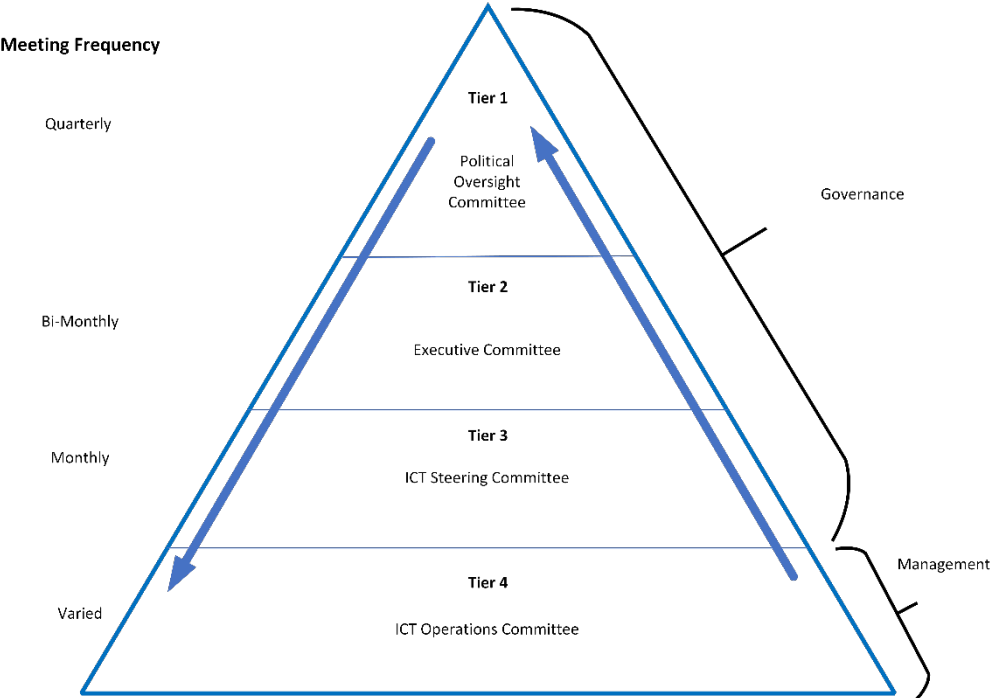


Figure 3.1: The CoT Corporate Governance Structure

3.3.1 Governance

The governance section of the diagram consists of three tiers made up of governance committees that meet on prearranged frequencies. These committees are the Political Oversight Committee, the Executive Committee and the ICT Steering Committee as discussed briefly in the respective sections that follow.

Political Oversight Committee

This committee's main responsibility is to evaluate the current business strategic goals and future use of ICT, by directing the preparation and implementation of plans to ensure that the use of ICT meets the business needs, which when implemented must be monitored for performance and conformance purposes to ensure that CoT's strategic goals are achieved. The committee meets on a quarterly basis as reflected in the diagram.

Executive Committee

This committee is responsible for aligning the ICT strategy business priorities to overall business objectives. The committee also decides on the highest priority ICT risk issue, and finally sets ICT overall investment and provides directional guidance. This committee meets on bi-monthly basis.

ICT Steering Committee

The third tier of the structure reflects the ICT Steering Committee which conceptualizes and oversees the alignment of IT strategy and that of the city as guided by the Corporate Governance of Information Communication Technology (CGICT) framework. The primary role of the committee is to conceptualize and oversee CGICT, ICT and strategic alignment. It coordinates and oversees the planning, implementation, and execution of the CGICT, ICT and strategic alignment and related monitoring activities. This committee meets on monthly basis to deliberate on matters as per its mandate. Page 20 of the CoT's ICT Governance Framework outlines the responsibilities of the ICT Steering Committee, chaired by the governance and support officer, provides strategic ICT leadership in the City of Tshwane (CoT) as follows:

- Develop corporate level ICT strategies and plans that ensure the cost-effective application and management of ICT systems and resources throughout the Municipality.
- Coordinate planning based on direction received from the Executive Committee (EXCO).
- Determine, prioritise, and recommend plans, policies, strategies, resource/capacity requirements, portfolios of ICT projects and risk man-

agement to EXCO.

- Oversee the implementation of approved ICT plans, policies, strategies, resource/capacity requirements, risk management, benefits realisation, portfolios of ICT projects, internal and external audits.
- Monitor and evaluate ICT projects and achievements against the ICT Strategic Plan.
- Coordination and alignment on City-Wide Smart City and Safe City initiatives/projects.
- Review current and future technologies to identify opportunities to increase the efficiency of ICT resources.
- Determine the monitoring criteria and related reporting requirements and processes for conformance, performance, and assurance.
- Take action to ensure that the ICT projects are delivered within the agreed budget and timeframe.
- Provide direction to all ICT related decisions that may have an impact on the business operations and culture of the department that is escalated to the committee.
- Determine the change management requirements for the implementation of CGICT and report to EXCO.
- Inform and make recommendations to the City manager and Council of the Municipality on significant ICT issues.
- Ensuring open communication between ICT and other functional units within the city. (Source)

3.3.2 Management

The management phase is made up of one committee which forms that 4th tier of the ICT governance structure of the CoT. As guided by COBIT standards, the committee looks at implementing decisions discharged by the top three committees at an operational level.

IT Operations Committee

This committee's primary responsibility is to operate and govern ICT as a business at an operational level.

3.3.3 Governance of the TFPM

As stated in the introduction of this study, the Tshwane Fresh Produce Market (TFPM) is a division under the Department of Economic Development and Spatial Planning (EDSP) within the CoT. The CoT has a Shared Service department headed by the Chief Information Officer (CIO) with the main responsibility of this individual being steering the organisation with regard to Information and Information Technology governance. In this context, the CoT's CIO takes the responsibility and accountability as the POPIA Information/Compliance Officer for the city. At the division level, the TFPM has a Divisional Head responsible for the development of operational procedure regarding collection, processing and safeguarding of personal information guided by the CoT's IT governance framework. The Divisional Head is assisted by the IT Manager responsible for overseeing systems that are used to collect, process and store personal information. In this context, the Divisional Head is responsible for POPIA compliance.

TFPM IT Governance Structure

Figure 3.2 below describes the governance structure of TFPM and its relationship with that of CoT. The structure reflects the accountable, responsible parties together with the operational roles of the IT sections at implementation level. The governance structure in Figure 3.2 shows the link that exists between the CoT's ICT governance structure and the operations of IT at the divisional level (TFPM level). The Divisional Head of the TFPM is a member of the CoT's ICT Steering Committee and a chair of TFPM's IT Steering Committee. The role's main responsibility is to implement the ICT strategic decisions made by the CoT's ICT Steering Committee.

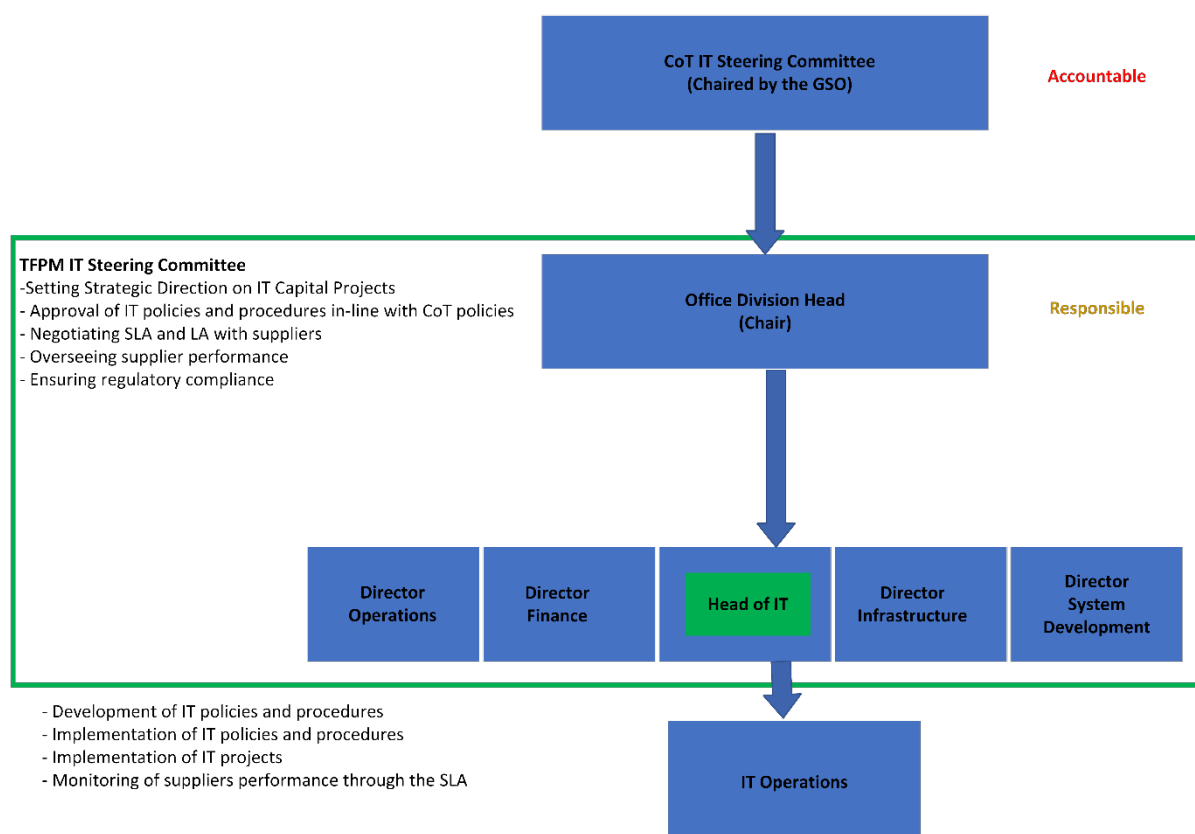


Figure 3.2: TFPM ICT Governance Structure

Amongst the CoT's strategic objectives is compliance to regulatory and regulative requirements. With POPIA being a regulative requirement, it therefore becomes the responsibility of the GSO to ensure compliance to it at the CoT level and the responsibility of the Divisional Head to ensure similar compliance at the divisional level. The subsequent section discusses a content analysis of the documents that govern the operations of both the CoT and the TFPM and therefore have a bearing on the personal information handling conduct of these entities.

3.4 Content Analysis

Content analysis is regarded as a flexible technique for analysing textualized data (Hsieh & Shannon, 2005). Bryman (2011) defines the content analysis process as a methodology that analyses documents, transcripts, interviews, text, audio, and video content in a detailed construed manner. Elo and

Kyngas (2008) , define two approaches to content analysis, namely inductive content analysis and deductive content analysis. The former is reportedly used where there is fragmented knowledge about a phenomenon. The latter is recommended where the analysis is based on prior knowledge and the purpose of the study is theory testing. Further, a deductive content analysis is believed to be based on an earlier theory or model. For the purposes of this study, a deductive approach to the content analysis was followed. Although Elo and Kyngas (2008), report that there are no systematic rules for analysing data, these authors define three phases for conducting a content analysis. The three phases of conducting a content analysis according to Elo and Kyngas (2008) are discussed in context of the study.

3.4.1 Preparation Phase

The first phase is the preparation phase, where the subject of analysis is identified. This includes determining the sample of data to be analysed (Elo & Kyngas, 2008). In this study, standard operating procedures (SOPs), service level agreements (SLAs) in the TFPM and the IT governance framework of the CoT were selected. The IT governance framework of the CoT has an influence on the business conduct of the TFPM IT operations.

3.4.2 Analysis Criteria

To conduct a deductive content analysis, a categorisation matrix is developed. This is the second phase. A categorisation matrix is generally based on earlier work or existing models or theories and is used to categorise and code data for the analysis. After developing a categorisation matrix, all the data is reviewed for content and coded to correspond with the identified categories (Elo & Kyngas, 2008). In the context of POPIA compliance, the Information Regulator has developed POPIA compliance guidelines in line with Chapter 3 of the protection of personal information act (POPIA) of 2013 (The Presidency, 2013). These guidelines are mainly linked or informed by the eight conditions that are detailed in the third chapter of the legislation. Although, the guidelines exist, there is still a need that organisations operationalise requirements outlined in the guidelines in alignment with their structures to ensure compliance. Nexia International, is an audit-

ing and accounting firm with extensive experience and expertise in various related disciplines including POPIA. The Nexia is highly regarded by both local and international business communities, fulfilling the role of auditors and consultants in various accounting and financial fields. Nexia's POPIA compliance checklist was used as the categorisation matrix for this study as the checklist contains various questions aligned to each of the eight POPIA conditions.

Compliance Checklist

Table 3.1 below shows a Nexia compliance checklist containing 15 questions that depict the broader aspects of POPIA requirements including the eight POPIA conditions of the POPI Act highlighted in Chapter 3. The 15 questions cover all the important elements an organisation should comply with as dictated by the legislation. This checklist was used with additional information to analyse the standard operating procedures (SOPs), service level agreements (SLAs) in the TFPM and the IT governance framework of the CoT for compliance with POPIA. The additional columns reflect the content's relevance to specific POPIA conditions, its applicability and whether there is compliance or non-compliance. In this way the researcher can make a decision based on the compliance status on each of the stated conditions.

Table 3.1: POPIA Compliance Checklist (Nexia, 2020)

No.	POPIA Statement	Related POPIA Condition
1	Does the company take all reasonable steps to prevent personal information being lost or damaged or unlawfully accessed and modified? (Companies should analyse their internal processes used to collect, record, retain, disseminate, and destroy personal information. Companies must ensure the integrity and safekeeping of personal information in their possession or under their control)	Process Limitations, Security Safeguard.
2	Is the purpose of the collection and processing of the personal information clearly set out and defined in company processes? Personal information must, in other words, be collected for a specific, explicitly defined, and lawful purpose that is related to a function or activity of the specific company. Transparency is imperative.	Purpose Specification
3	Does your company process personal information in an adequate, relevant, and non-excessive manner, given the purpose it is processed for? The processing of personal information should always be limited.	Further Processing
4	Is the individual whose personal information is collected and processed informed thereof? The individual should be made aware of the details of the company processing their information and in addition the individual must be informed as to whether the processing of their information is voluntary or for mandatory reasons.	Openness
5	Will the company further process the personal information? The reasons (if any) for further processing of personal information should be clearly communicated to the individual it is collected from and further processing must be related to the purpose for which the information was initially collected	Further Processing
6	Is the personal information of individuals available and easily accessible by relevant role-players within the company? Personal information should be available to identified role-players for them to retrieve such information immediately.	Data Subject Participation
7	Does the company empower employees through training to work responsibly with personal information? Pro-active measures should be taken to influence and guide employees to work responsibly with and protect personal information.	Security and Safeguard
8	Has the company considered protection of the integrity and quality of the personal information? The company processing the information must always ensure that the information is complete, accurate, up to date and not misleading.	Information Quality

9	Has the company appointed an Information Officer (IO) and is the IOs appointment registered with the Information Regulator? Companies are obliged to register a duly appointed Information Officer with the Information Regulator whose responsibility it is to work with and notify the Regulator of any request or complaint in terms of POPIA.	Accountability
10	Does the company have a POPIA Compliance Framework? All companies should consider prioritizing drafting a POPIA Compliance Framework. The IO should also ensure that this is developed, implemented, and monitored.	All Conditions
11	Is there a process that individuals can follow to request details of the personal information held by the company? POPIA allows individuals to make certain requests, free of charge, to companies in possession of their personal information. For instance, an individual has the right to know the identity of all third parties that have had access to their information. Further, any person whose information is being processed by a company may ask for a full record of the information held by such a company.	Openness, Data subject participation.
12	Does the company have a Retention of Records Policy, or a Retention Schedule incorporated in the Data Retention Policy? Personal information must be destroyed, deleted, or destructed as soon as the purpose for collecting the information has been achieved by the company. Retention of records' schedules should be drafted with legislation, industry rules and regulations and good practice in mind.	Purpose Specification
13	Will the company transfer personal information over borders? There are certain restrictions on the sending of personal information out of South Africa and back into South Africa. The applicable restrictions will depend on the laws of the country to whom the data is transferred or from where the data is returned.	Further Processing
14	Has the company's Information Governance Maturity been assessed? To determine the current versus ideal state of POPIA Compliance it is recommended that the company assess its Information Governance Maturity.	Accountability
15	Does the company have a Privacy Notice? An easy-to-understand Privacy Notice should be drafted and available for every company collecting and processing personal information of individuals.	Accountability

Sampling Documentation and Data Analysis

The third phase of the content analysis process describes the analysis of data that fits the categories of the matrix. Only that content which is applicable to the purpose of the study should be analysed (Elo & Kyngas, 2008). Table 3.2 below describes the four documents that have been evaluated to test compliance with POPIA conditions using the Nexia compliance checklist. The table reflects the name of the document, the content that was focused on and the responsible governance structure as per the CoT and TFPMs corporate and IT governance structures.

Table 3.2: Summary of Analysed Documentation

Available Document	Content Analysed	Responsible Governance Structure
Buyer Registration Procedure (TFPM)	Compliance to consent to aspects of POPIA and the legality element in collecting personal information.	TFPM Structure (Finance Directorate)
Service Level Agreement with Fresh mark Systems (TFPM)	The service level agreement (SLA) clauses that are in line with any condition of POPIA on collection, handling, and storage of personal information.	TFPM Structure (ICT Directorate)
Fresh-mark Systems License Agreement (TFPM)	The License agreement (LA) clauses that are in line with any condition of POPIA on collection, handling, and storage of personal information.	TFPM Structure (ICT Directorate)
Information Technology Governance Framework (CoT)	Assessment of procedure, policies, strategies, and processes that are incorporated into the ICT Governance framework in line with the POPIA requirement.	CoT Governance Structure (ICT Steering Committee)

3.5 Buyer Account Registration Procedure (SOP)

The buyers account registration procedure defines the process followed for opening a buyers account related to Cash Management services and Revenue

Management (when purchasing on credit). The document scope is limited to the TFPM only and is not city wide. There are no review intervals specified in this document.

Registration Process

This SOP was developed in April 2015 and has not been revised to date given its relevance to the current market operations. The SOP states that during the registration process, a prospective buyer is provided with a registration form where all necessary personal information such as name, surname, ID number, proof of residential address, bank account number and date of birth are completed; the form is then collected by the market before processing. In addition to the personal information of the account holder, the form further requires that the account holder provides personal information of sub-account holders. These are persona that the account holder may request to purchase or perform other transactions on their behalf. Their personal information also involves Identity number, residential address, name and surname and signature. Accompanying the registration form is an indemnity/consent form which highlights that the account holder will be held responsible for any activities performed on their account and that the city of Tshwane or the TFPM will not be held liable for claims, demands, actions, suites, costs, and damages as a result of fraudulent activities, with the reason being that personal information may be accessed by unauthorised people due to negligence by the account holder. The form and the consent statement do not in any way amplify the purpose of collection of personal information and further to that, it does not allow the account holder to consent to collection and processing of their personal information.

Condition Compliance Test

This document is aligned to the Accountability condition as described in section 8 of the POPI act, and it outlines that is it the responsibility of the organisation to ensure that laws set out in this legislation are complied with. To ensure compliance with Information Technology governance (ITG) and any information laws, the city has appointed the Chief Information Officer (CIO) to ensure that laws and regulations are adhered to through the development and implementation of relevant operational policies. The CIO

becomes accountable for any action related to information and information technology. It is the responsibility of the CIO to ensure that processing of personal information is not done in any way other than for the purpose stated during the personal information collection stage. Although it is not stated in the TFPM buyer registration SOP, the above assessment reflects that the city and the market are complying with the accountability condition of the POPI act through the responsibilities vested in the CIO and the TFPM Management. The issue noted in the SOP is that in the case of indemnity, the Market does not want to be held accountable for any personal information breaches or any unauthorised access to the buyer s personal information.

The document further leans towards sections 9,10,11 and 12 of the POPI act described by the Processing Limitation condition. This condition is categorized into four critical elements that must be complied with to meet the full requirements of the condition. The first element of the condition is linked to condition one by briefly stating the importance of lawful collection and processing of personal information in a manner that does not infringe on the privacy of the personal information owner. The second element speaks to minimality, which states that personal information may only be processed provided the purpose for processing is adequate, relevant, and not excessive. Taking a close look at the buyers registration procedure SOP, the document does not reflect or make any reference to regulative element about collection and processing of buyers personal information. The document also does not clearly outline the purpose for collection of personal information and does not in any way reflect a process of ensuring that privacy of the personal information is not infringed. The third aspect of this condition speaks about the consent, justification, and objection. Although there is a disclaimer clause in the indemnity section of the SOP, elements of consent, justification and objection by the personal information owner are not covered, which make the SOP non-compliant with this aspect of condition 2. The condition further states that personal information must be collected directly from the owner except under the circumstances outlined under subsection 2 of section 12 of this condition. Although it is not outlined in the process, during the process of buyer registration, the registration form requiring personal information is provided directly to the personal information owner and on completion is returned directly to the market for capturing. This process entails that

personal information is collected directly from the owner with no exceptions.

Another condition that focuses on two aspects that must be complied with by the personal information collector and processor aligned to this document is the Purpose Specification condition. The first aspect expresses that personal information being collected for a purpose explicitly defined, is lawful and related to the primary functions of the responsible party while the second aspect outlines the retention and restriction of records policies. Although personal information is lawfully collected from the owner for the function related to operations of TFPM, as stated in condition 2, the TFPM's buyers registration SOP does not clearly identify the purpose of collecting the personal information to buyers, which is a major shortfall of the SOP. Another shortfall is that the TFPM does not have a policy on the retention and restriction of records of personal information.

Table 3.3: Buyers Registration SOP Compliance Test

No.	POPIA Statement	Related POPIA Condition	Applicable?	Compliant?
1	Does the company take all reasonable steps to prevent personal information being lost or damaged or unlawfully accessed and modified? (Companies should analyse their internal processes used to collect, record, retain, disseminate, and destroy personal information. Companies must ensure the integrity and safekeeping of personal information in their possession or under their control).	Process Limitations, Security Safeguard.	N/A	N/A
2	Is the purpose of the collection and processing of the personal information clearly set out and defined in company processes? Personal information must, in other words, be collected for a specific, explicitly defined, and lawful purpose that is related to a function or activity of the specific company. Transparency is imperative.	Purpose Specification	Y	N
3	Does your company process personal information in an adequate, relevant, and non-excessive manner, given the purpose it is processed for? The processing of personal information should always be limited.	Further Processing	N/A	N/A
4	Is the individual whose personal information is collected and processed informed thereof? The individual should be made aware of the details of the company processing their information and in addition the individual must be informed as to whether the processing of their information is voluntary or for mandatory reasons.	Openness	Y	N

5	Will the company further process the personal information? The reasons (if any) for further processing of personal information should be clearly communicated to the individual it is collected from and further processing must be related to the purpose for which the information was initially collected.	Further Processing	Y	N
6	Is the personal information of individuals available and easily accessible by relevant role-players within the company? Personal information should be available to identified role-players for them to retrieve such information immediately.	Data Subject Participation	Y	Y
7	Does the company empower employees through training to work responsibly with personal information? Pro-active measures should be taken to influence and guide employees to work responsibly with and protect personal information.	Security and Safeguard	Y	Y
8	Has the company considered protection of the integrity and quality of the personal information? The company processing the information must always ensure that the information is complete, accurate, up to date and not misleading.	Information Quality	Y	Y

9	<p>Has the company appointed an Information Officer (IO) and is the IOs appointment registered with the Information Regulator? Companies are obliged to register a duly appointed Information Officer with the Information Regulator whose responsibility it is to work with and notify the Regulator of any request or complaint in terms of POPIA.</p>	Accountability	N/A	N/A
10	<p>Does the company have a POPIA Compliance Framework? All companies should consider prioritizing drafting a POPIA Compliance Framework. The IO should also ensure that this is developed, implemented, and monitored.</p>	All	Y	N
11	<p>Is there a process that individuals can follow to request details of the personal information held by the company? POPIA allows individuals to make certain requests, free of charge, to companies in possession of their personal information. For instance, an individual has the right to know the identity of all third parties that have had access to their information. Further, any person whose information is being processed by a company may ask for a full record of the information held by such a company.</p>	Openness, Data Subject Participation.	Y	N
12	<p>Does the company have a Retention of Records Policy, or a Retention Schedule incorporated in the Data Retention Policy? Personal information must be destroyed, deleted, or destructed as soon as the purpose for collecting the information has been achieved by the company. Retention of records schedules should be drafted with legislation, industry rules and regulations and good practice in mind.</p>	Purpose Specifications	Y	N

13	Will the company transfer personal information over borders? There are certain restrictions on the sending of personal information out of South Africa and back into South Africa. The applicable restrictions will depend on the laws of the country to whom the data is transferred or from where the data is returned	Further Processing	N/A	N/A
14	Has the company's Information Governance Maturity been assessed? To determine the current versus ideal state of POPIA Compliance it is recommended that the company assess its Information Governance Maturity.	Accountability	N/A	N/A
15	Does the company have a Privacy Notice? An easy-to-understand Privacy Notice should be drafted and available for every company collecting and processing personal information of individuals.	Accountability	Y	N
Compliance percentage				30%

Summary: Studying Table 3.3, out of the 15 elements t in the questionnaire, 10 are applicable to the analysed process and out of the 10, the process is compliant to only 3 aspects making this is only 30% compliant to POPIA conditions.

3.6 License Agreement (Between TFPM and Fresh-mark Systems)

A licensing agreement is a contract between two parties in which the licensor grants the licensee the right to use the brand name, trademark, patented technology, or ability to produce and sell goods owned by the licensor (Team, 2022). The purpose of the license agreement between the TFPM and the FMS is to outline conditions of the relationship between the two parties within the scope of the law of the Republic while highlighting the annual cost that the TFPM will incur for the utilization of the FMS s system software. This

document is reviewed annually by the FMS and TFPM in line with assurance requirements.

3.6.1 Condition Compliance Test

This document touches on elements of condition 4 of the POPI act. The condition requires that further processing of information be compatible with the initial purpose of the collection as set out in section 13 of the Act. The condition outlines five requirements that must be taken into cognizance to determine the compatibility of the initial purpose of collection and that of intended further processing. These five requirements are as follows:

- Take account of the purpose of the intended further processing and that of the initial collection.
- Take account of the nature of information collected.
- Check consequences of the intended further processing on the data owner.
- Take note of the way personal information is collected.
- Take cognizance of the contractual rights and agreement between parties.

In the context of the TFPM, further processing of personal information takes place through the agreement between the TFPM and Fresh-mark systems (The service provider). Fresh-mark system being the service provider, has access to personal information collected by the TFPM for further processing in line with the initial purpose of collection by the TFPM. To lawfully conduct further processing of personal information, the TFPM and Fresh-mark systems have a license agreement in place outlining the conditions of processing personal information by Fresh-mark systems as the third party. Because the TFPM does not hold any document that reflects the purpose of collecting the personal information from buyers, it becomes difficult to test the compatibility of the initial processing purpose and further processing displayed on the license agreement. Having analysed the license agreement, the purpose displayed in it is clear although it is not in accordance with any initial purpose as required by clause (a) of subsection 2 of condition 4. The

nature of the information that is furtherly processed by Fresh-mark systems is in line with what was collected by the TFPM as required by clause (b) of subsection 2 of condition 4. The agreement further reflects elements that might have consequences to the personal information owner through its confidentiality clause as quoted below: Except as otherwise provided, each party undertakes to retain in confidence all information and know-how transmitted or disclosed to the other that the disclosing party has identified as being proprietary and/or confidential or that, by the nature of the circumstances surrounding the disclosure, ought to be treated as proprietary and/or confidential, and undertakes not to use such information and know-how except under the terms and during the existence of this agreement. This clause is in the best interest of the personal information owner in the sense that it prioritizes confidentiality of their personal information by holding both parties accountable. The condition further advises that cognizance be taken on the way personal information is collected. Although it is not reflected in the agreement or any documentation within the TFPM, personal information is collected manually using paper-based forms. It is then electronically captured into the Fresh-mark system for processing by both the TFPM and Fresh-mark systems. Finally, the condition advises the importance of taking cognizance of the contractual agreement between TFPM and Fresh-mark Systems or the processing and organisation and the further processing. Having analysed the agreement document, it is clear that annual reviews of the agreement are performed to scrutinize the contents of the agreement which are in line with clause (e) of subsection 2 of condition 4.

Table 3.4: License Agreement Compliance Test

No.	POPIA Statement	Related POPIA Condition	Applicable?	Compliant?
1	Does the company take all reasonable steps to prevent personal information being lost or damaged or unlawfully accessed and modified? (Companies should analyse their internal processes used to collect, record, retain, disseminate, and destroy personal information. Companies must ensure the integrity and safekeeping of personal information in their possession or under their control).	Process Limitations, Security Safeguard.	Y	Y
2	Is the purpose of the collection and processing of the personal information clearly set out and defined in company processes? Personal information must, in other words, be collected for a specific, explicitly defined, and lawful purpose that is related to a function or activity of the specific company. Transparency is imperative.	Purpose Specification	N/A	N/A
3	Does your company process personal information in an adequate, relevant, and non-excessive manner, given the purpose it is processed for? The processing of personal information should always be limited.	Further Processing	Y	Y
4	Is the individual whose personal information is collected and processed informed thereof? The individual should be made aware of the details of the company processing their information and in addition the individual must be informed as to whether the processing of their information is voluntary or for mandatory reasons.	Openness	N/A	N/A

5	Will the company further process the personal information? The reasons (if any) for further processing of personal information should be clearly communicated to the individual it is collected from and further processing must be related to the purpose for which the information was initially collected.	Further Processing	Y	Y
6	Is the personal information of individuals available and easily accessible by relevant role-players within the company? Personal information should be available to identified role-players for them to retrieve such information immediately.	Data Subject Participation	Y	Y
7	Does the company empower employees through training to work responsibly with personal information? Pro-active measures should be taken to influence and guide employees to work responsibly with and protect personal information.	Security and Safeguard	Y	N
8	Has the company considered protection of the integrity and quality of the personal information? The company processing the information must always ensure that the information is complete, accurate, up to date and not misleading.	Information Quality	Y	Y

9	<p>Has the company appointed an Information Officer (IO) and is the IO's appointment registered with the Information Regulator? Companies are obliged to register a duly appointed Information Officer with the Information Regulator whose responsibility it is to work with and notify the Regulator of any request or complaint in terms of POPIA.</p>	Accountability	N/A	N/A
10	<p>Does the company have a POPIA Compliance Framework? All companies should consider prioritizing drafting a POPIA Compliance Framework. The IO should also ensure that this is developed, implemented, and monitored.</p>	All Conditions	Y	Y
11	<p>Is there a process that individuals can follow to request details of the personal information held by the company? POPIA allows individuals to make certain requests, free of charge, to companies in possession of their personal information. For instance, an individual has the right to know the identity of all third parties that have had access to their information. Further, any person whose information is being processed by a company may ask for a full record of the information held by such a company.</p>	Openness, Data Subject Participation.	Y	Y
12	<p>Does the company have a Retention of Records Policy, or a Retention Schedule incorporated in the Data Retention Policy? Personal information must be destroyed, deleted, or destructed as soon as the purpose for collecting the information has been achieved by the company. Retention of records schedules should be drafted with legislation, industry rules and regulations and good practice in mind.</p>	Purpose Specifications	Y	N

13	Will the company transfer personal information over borders? There are certain restrictions on the sending of personal information out of South Africa and back into South Africa. The applicable restrictions will depend on the laws of the country to whom the data is transferred or from where the data is returned	Further Processing	N/A	N/A
14	Has the company's Information Governance Maturity been assessed? To determine the current versus ideal state of POPIA Compliance it is recommended that the company assess its Information Governance Maturity.	Accountability	N/A	N/A
15	Does the company have a Privacy Notice? An easy-to-understand Privacy Notice should be drafted and available for every company collecting and processing personal information of individuals.	Accountability	Y	Y
Compliance percentage				80%

Summary: Studying Table 3.4, the compliance assessment results of the SLA document between the TFPM and FMS, 10 aspects of the questionnaire are applicable to the SLA and of the 10 aspects, eight are found to be compliant with POPIA requirements making the document 80% compliant with POPIA conditions.

3.7 Service Level Agreement (SLA) (Between TFPM and Fresh-mark Systems)

Mirobi and Arockiam (2015), define the Service Level Agreement as a contract, contracted between provider of the service and the third party such as purchaser of service, dealer(agent) or monitor(agent), where service is formally defined. Therefore, it is utmost important that organisations have clearly defined SLAs with third parties to avoid disastrous consequences in the customer business (Badshah, Ghani, Shamshirband, Aceto, & Pescapè,

2020). In the context of this study an SLA may also be used to cover some aspects of policies, legislative and regulatory requirements. The purpose of the SLA between the TFPM and FMS is to outline the standard of service that the offering party (FMS) will be rendering to the receiving party (TFPM).

3.7.1 SLA Content Discussion

This SLA is aligned to the annual licence agreement which the two parties sign, but it clarifies details about the Mean Time to Respond (MTTR) by the FMS on requests, projects, and incidents that the TFPM report on in its daily operations. The document clearly defines the scope of the agreement and further indicates the roles and responsibilities of each party. Although the document does not display a dedicated process for accessing or reporting of personal information breaches, it has in place a process to report requests and incidents which might also be used for reporting of personal information activities. The document further outlines the process to be engaged when reporting on performance and availability of systems where personal information is processed and stored. Importantly, the document has a confidentiality clause in place stating how personal information must be acted upon by the two parties to ensure confidentiality. Below are conditions of the confidentiality clause as outlined in the SLA:

- (a) The Parties agree that the terms of this Agreement and all Confidential Information of the Parties communicated to them in connection with this Agreement will be received in such form as particularity required and used only for the purposes of this Agreement. Each Party will use the same means as it uses to protect its own confidential information, but in no event less than reasonable means, to prevent the disclosure and to protect confidentiality of such Confidential Information.
- (b) No confidential information received by any of the Parties (“the Recipient Party”) will be disclosed by the Recipient Party, its agents, representatives, or employees without the prior written consent of the other Party, such consent shall not be unreasonably withheld or delayed.
- (c) The provisions of this clause do not apply to information which is:

- (i) publicly known or becomes publicly known through no unauthorised act of the Recipient Party.
- (ii) rightfully received by the Recipient Party from a third party.
- (iii) independently developed by the Recipient Party without use of any other Party's information.
- (iv) required to be disclosed pursuant to a requirement of any relevant Stock Exchange or Government agency regulation or rule, or any applicable law, provided always that the Party required to disclose the Confidential Information (the Disclosing Party) gives the other Party reasonable prior notice to such a disclosure being made.

3.7.2 Condition Compliance Test

This is a condition with brief, but critical compliance requirements. Its primary focus is on quality and integrity of personal information produced through processing and further processing operations. It states it is the responsibility of the processing party to ensure that personal information is accurate, complete, and not misleading. The condition further highlights that the processing party must ensure that personal information is updated where necessary and that cognizance must be taken that there is no deviation from the purpose of collection and further processing thereof. To maintain the quality of data including personal information, Clause 12 of the Service Level Agreement (SLA) between the TFPM and the Fresh-mark System states that no confidential information received by any of the Parties (the Recipient Party) will be disclosed by the Recipient Party, its agents, representatives or employees without the prior written consent of the other Party, such consent shall not be unreasonably withheld or delayed with the exclusion of information that is :

- Publicly known or becomes publicly known through no unauthorized act of the Recipient Party.
- Rightfully received by the Recipient Party from a third party.
- Independently developed by the Recipient Party without use of any other Party's information.

- Required to be disclosed pursuant to a requirement of any relevant Stock Exchange or Government agency regulation or rule, or any applicable law, provided always that the Party required to disclose the Confidential Information (the Disclosing Party) gives the other Party reasonable prior notice to such a disclosure being made.

Further in compliance with this condition, the SLA highlights an important statement about accuracy and integrity of personal information processed by the two parties as quoted below: While TM strives to ensure the accuracy of all material, the ultimate responsibility of checking copy and proofs remains with FMS, who will have no recourse to TM in the event of discrepancies in the final product save for circumstances wherein TM has provided incorrect information to FMS which has had an adverse effect in rendering the Services. This clause has been included in the SLA to ensure integrity and accuracy of personal information. Section 17 of the POPI act describes requirements under condition 6. The condition states that it is the responsibility of the processing party to ensure the maintenance of the collection and processing documentation as referred to in section 14 of the Promotion of Access to Information Act (PAIA). The condition further outlines aspects of notification to personal information owners whenever their information is collected. Section 18 subsection 1(a) to 3(f) highlights details requirements that should be met regarding notification to personal information owner when collecting their data. On maintenance of the personal information processing documentation, the TFPM last reviewed its buyer registration SOP in April 2015, and it is evident that maintenance of this documentation is not performed annually as per governance standards. The documentation for processing is contained in the License Agreement (LA) and Service Level Agreement (SLA) administered by Fresh Mark Systems and is reviewed accordingly on an annual basis. Additional to the LA and SLA, Fresh Mark System has developed processing documentation in alignment with the protection of personal information act (POPIA) which will be maintained on annual basis going forward.

Table 3.5: Service Level Agreement Compliance Test

No.	POPIA Statement	Related POPIA Condition	Applicable?	Compliant?
1	Does the company take all reasonable steps to prevent personal information being lost or damaged or unlawfully accessed and modified? (Companies should analyse their internal processes used to collect, record, retain, disseminate, and destroy personal information. Companies must ensure the integrity and safekeeping of personal information in their possession or under their control).	Process Limitations, Security Safeguard.	Y	Y
2	Is the purpose of the collection and processing of the personal information clearly set out and defined in company processes? Personal information must, in other words, be collected for a specific, explicitly defined, and lawful purpose that is related to a function or activity of the specific company. Transparency is imperative.	Purpose Specification	Y	N
3	Does your company process personal information in an adequate, relevant, and non-excessive manner, given the purpose it is processed for? The processing of personal information should always be limited.	Further Processing	Y	Y
4	Is the individual whose personal information is collected and processed informed thereof? The individual should be made aware of the details of the company processing their information and in addition the individual must be informed as to whether the processing of their information is voluntary or for mandatory reasons.	Openness	Y	N

5	Will the company further process the personal information? The reasons (if any) for further processing of personal information should be clearly communicated to the individual it is collected from and further processing must be related to the purpose for which the information was initially collected.	Further Processing	Y	Y
6	Is the personal information of individuals available and easily accessible by relevant role-players within the company? Personal information should be available to identified role-players for them to retrieve such information immediately.	Data Subject Participation	Y	Y
7	Does the company empower employees through training to work responsibly with personal information? Pro-active measures should be taken to influence and guide employees to work responsibly with and protect personal information.	Security and Safeguard	N/A	N/A
8	Has the company considered protection of the integrity and quality of the personal information? The company processing the information must always ensure that the information is complete, accurate, up to date and not misleading.	Information Quality	Y	Y
9	Has the company appointed an Information Officer (IO) and is the IOs appointment registered with the Information Regulator? Companies are obliged to register a duly appointed Information Officer with the Information Regulator whose responsibility it is to work with and notify the Regulator of any request or complaint in terms of POPIA.	Accountability	N/A	N/A

10	Does the company have a POPIA Compliance Framework? All companies should consider prioritizing drafting a POPIA Compliance Framework. The IO should also ensure that this is developed, implemented, and monitored.	All Conditions	Y	N
11	Is there a process that individuals can follow to request details of the personal information held by the company? POPIA allows individuals to make certain requests, free of charge, to companies in possession of their personal information. For instance, an individual has the right to know the identity of all third parties that have had access to their information. Further, any person whose information is being processed by a company may ask for a full record of the information held by such a company.	Openness, Data Subject Participation.	Y	N
12	Does the company have a Retention of Records Policy, or a Retention Schedule incorporated in the Data Retention Policy? Personal information must be destroyed, deleted, or destructed as soon as the purpose for collecting the information has been achieved by the company. Retention of records schedules should be drafted with legislation, industry rules and regulations and good practice in mind.	Purpose Specifications	Y	N

13	Will the company transfer personal information over borders? There are certain restrictions on the sending of personal information out of South Africa and back into South Africa. The applicable restrictions will depend on the laws of the country to whom the data is transferred or from where the data is returned	Further Processing	N/A	N/A
14	Has the company's Information Governance Maturity been assessed? To determine the current versus ideal state of POPIA Compliance it is recommended that the company assess its Information Governance Maturity.	Accountability	N/A	N/A
15	Does the company have a Privacy Notice? An easy-to-understand Privacy Notice should be drafted and available for every company collecting and processing personal information of individuals.	Accountability	Y	N
Compliance percentage				45%

Summary: Of the 15 elements that are outlined in the checklist (Table 3.5), 11 were found to be applicable to the tested License Agreement (LA). Out of the 11 elements, the process reflected it to be compliant for only five aspects resulting in it being only 45% compliant with POPIA requirements.

3.8 IT Governance Framework (CoT)

As highlighted in the document, the purpose of this ICT Policy Framework is to be institutionalized as an integral part of corporate governance within city. This framework provides the political and executive leadership with a set of principles and practices that must be complied with as well as the implementation approach to be used for corporate governance of ICT within the city's ICT department. As described in this document, the IT Governance Framework ensures that CoT objectives are achieved by evaluating stakeholder needs, conditions, and options; setting direction through prioritization

and decision making; and monitoring performance, compliance and progress against agreed-on direction and objectives.

3.8.1 Document Discussion

The CoT's IT Governance Framework document is incorporated into the city's Corporate Governance Framework together with the following documentation: The IT Strategy, The Information Security Policy, IT Governance Framework, Project Management Guidelines, and the Change Management Process. Only the area that reviews the handling and storing of personal information in this document are evaluated. Development of the framework and its contents are mainly informed by the IT governance standards below as outlined in the document:

Table 3.6: CoT IT Governance Framework

King III/King IV	This most accepted corporate governance framework in South Africa is also valid for the public service. It was used to inform the corporate governance of ICT principles and practices in this Policy no: ICT-FW01 Effective from: 1 April 2018 Page number: 1-27 Policy: ICT Governance Framework Page 4 document and to establish the relationship between corporate governance of ICT and governance of ICT (Modiha, 2018).
ISO/IEC 38500	This standard is internationally accepted as the standard for corporate governance of ICT; it provides governance principles and a model (Juiz et al., 2018).
ITIL	The Information Technology Infrastructure Library (ITIL) aims to identify best practices with regard to managing IT service levels and a number of organisations (Dugmore & Sharon, 2008).
COBIT	This is an internationally accepted process framework for implementing governance of ICT. COBIT fully supports the principles of the King III Code and the ISO/IEC 38500 standard in the corporate governance of ICT (De Haes et al., 2020).

In addition to the IT Governance standards of best practice, the document further refers to the following legislative and regulatory frameworks including POPIA:

Legislation	Act Number
Constitution of the Republic of South Africa	Act 108 of 1996
Copyright Act	Act 98 of 1978
Electronic Communications and Transactions Act	Act 25 of 2002.
Minimum Information Security Standards	Approved by Cabinet in 1996
Local Government: Municipal Finance Management Act	Act 56 of 2003
Local Government: Municipal Structures Act	Act 117 of 1998
Local Government: Municipal Systems Act	Act 32 of 2000
National Archives and Record Service of South Africa Act	Act 43 of 1996
Protection of Personal Information Act	Act 4 of 2013
Promotion of Access to Information Act	Act 2 of 2000
Regulation of Interception of Communications and Provision of Communication-related	Act 70 of 2002

Table 3.7: CoT IT Governance Framework Related Legislation and Regulations

When developing its IT Governance Framework, the city took into consideration all relevant legislations (Table 3.7) with POPIA included as the main regulative framework on which the study focuses.

3.8.2 Condition Compliance Test

The document outlines the city IT governance structure with the chairperson of the IT Steering Committee taking accountability for any activities related to IT as guided by Chapter 5 of the King III report of 2009. This aspect of the document is linked to the accountability condition of the POPI Act.

Governance Maturity Assessment

The document further highlights the importance of having a Governance Maturity Assessment in place. The documents states that city is currently in the process of developing or evolving their current ICT governance framework conducting an ICT governance maturity assessment to understand the environment being studied. The document further acknowledges that, Maturity Assessments should be conducted annually based on the functions within the organisation to determine gaps and produce a remediation plan to address these gaps. It is stated in the document that the city was at Maturity level 1 during the assessment conducted in 2013, which is the lowest level in terms

of the ICT Governance Maturity Model. This section of the document leans towards PART 2 of the POPI act, which does not necessarily form part of the eight conditions but part of the overall requirements of the POPI Act.

Information Technology Governance Measures

Outlined in the document are measures in place to address various Information Technology threats and to ensure business continuity as required by the Department of Public Services Administration's (DPSA)'s CGICT framework. The framework highlights the tools that each government entity should put in place to ensure smooth delivery of services delivered through the IT platforms and in compliance with regulative and regulatory requirements. Having most of these measures implemented by public service organisations including the TFPM will have a positive impact in complying with POPIA and its conditions as most measures are aligned with these requirements.

Table 3.8: Available IT Governance Measures

Measure	Description
Internal Audit Plan	The plan includes ICT audits. It also indicates how the internal audit function will be capacitated to perform ICT-related audits. This is informed by the National Treasury Internal Audit Framework and COBIT 5 Process MEA01 [9]
ICT Portfolio Management Framework	The framework is embedded in the departmental programme management structures. It explains how the department will create the necessary capacity to manage ICT-related business projects.
Information Plan and ICT Security Policy	The plan and policy ensure that classified information, intellectual property, and personnel information are protected within ICT systems
Disaster Recovery Plan	The plan is informed by the operational, information and data requirements of the business. This DRP informs the ICT Continuity Policy and Plan as outlined by COBIT 5.
Change Management Plan	Change management addresses the human behavioural and cultural aspects of the change. A structured and proactive approach should be followed to ensure acceptance and buy-in from the political and strategic leadership as well as the operational staff of the department. The change management plan includes training, communication, organisational design, and process redesign.
ICT Business Plan	The ICT Plan is an articulation of the business strategy and its related information into ICT requirements. It shows how ICT should enable business service delivery in a prioritized and measurable way and how its implementation will be monitored from a business perspective. The ICT Plan is a result of applying an enterprise architecture methodology.
Information Plan	The department's Information Plan ensures that agile and reputable information is available and managed to support the core and front-line service delivery. The Information Plan thus articulates the physical and electronic information needs of the department
Continuous Improvement Road Map	The successful implementation of a CGICT systems lead to continuous improvement. The continuous improvement process examines the effectiveness of the CGICT, POPIA and strategic alignment in order to identify areas of and opportunities for improvement. It should be measured through a maturity assessment methodology where shortcomings are addressed and articulated in a continuous improvement road map.

The information in Table 3.8 is taken as is from the City of Tshwane's ICT Governance Framework as a reflection of how some elements of ICT governance are conducted widely within the city.

Table 3.9: CoT ICT Governance Framework Compliance

No.	POPIA Statement	Related POPIA Condition	Applicable?	Compliant?
1	Does the company take all reasonable steps to prevent personal information being lost or damaged or unlawfully accessed and modified? (Companies should analyse their internal processes used to collect, record, retain, disseminate, and destroy personal information. Companies must ensure the integrity and safekeeping of personal information in their possession or under their control).	Process Limitations, Security Safeguard.	Y	Y
2	Is the purpose of the collection and processing of the personal information clearly set out and defined in company processes? Personal information must, in other words, be collected for a specific, explicitly defined, and lawful purpose that is related to a function or activity of the specific company. Transparency is imperative.	Purpose Specification	Y	Y
3	Does your company process personal information in an adequate, relevant, and non-excessive manner, given the purpose it is processed for? The processing of personal information should always be limited.	Further Processing	Y	Y

4	Is the individual whose personal information is collected and processed informed thereof? The individual should be made aware of the details of the company processing their information and in addition the individual must be informed as to whether the processing of their information is voluntary or for mandatory reasons.	Openness	N/A	N/A
5	Will the company further process the personal information? The reasons (if any) for further processing of personal information should be clearly communicated to the individual it is collected from and further processing must be related to the purpose for which the information was initially collected.	Further Processing	N/A	N/A
6	Is the personal information of individuals available and easily accessible by relevant role-players within the company? Personal information should be available to identified role-players for them to retrieve such information immediately.	Data Subject Participation	Y	Y
7	Does the company empower employees through training to work responsibly with personal information? Pro-active measures should be taken to influence and guide employees to work responsibly with and protect personal information.	Security and Safeguard	Y	Y
8	Has the company considered protection of the integrity and quality of the personal information? The company processing the information must always ensure that the information is complete, accurate, up to date and not misleading.	Information Quality	Y	Y

9	<p>Has the company appointed an Information Officer (IO) and is the IO's appointment registered with the Information Regulator? Companies are obliged to register a duly appointed Information Officer with the Information Regulator whose responsibility it is to work with and notify the Regulator of any request or complaint in terms of POPIA.</p>	Accountability	Y	Y
10	<p>Does the company have a POPIA Compliance Framework? All companies should consider prioritizing drafting a POPIA Compliance Framework. The IO should also ensure that this is developed, implemented, and monitored.</p>	All Conditions	Y	N
11	<p>Is there a process that individuals can follow to request details of the personal information held by the company? POPIA allows individuals to make certain requests, free of charge, to companies in possession of their personal information. For instance, an individual has the right to know the identity of all third parties that have had access to their information. Further, any person whose information is being processed by a company may ask for a full record of the information held by such a company.</p>	Openness, Data subject participation.	Y	Y
12	<p>Does the company have a Retention of Records Policy, or a Retention Schedule incorporated in the Data Retention Policy? Personal information must be destroyed, deleted, or destructed as soon as the purpose for collecting the information has been achieved by the company. Retention of records schedules should be drafted with legislation, industry rules and regulations and good practice in mind.</p>	Purpose Specifications	Y	Y

13	Will the company transfer personal information over borders? There are certain restrictions on the sending of personal information out of South Africa and back into South Africa. The applicable restrictions will depend on the laws of the country to whom the data is transferred or from where the data is returned	Further Processing	N/A	N/A
14	Has the company's Information Governance Maturity been assessed? To determine the current versus ideal state of POPIA Compliance it is recommended that the company assess its Information Governance Maturity.	Accountability	Y	Y
15	Does the company have a Privacy Notice? An easy-to-understand Privacy Notice should be drafted and available for every company collecting and processing personal information of individuals.	Accountability	Y	Y
Compliance percentage				92%

Summary: Looking at the assessment checklist (Table 3.9) above, out of the 15 elements the city's ICT Governance Framework is applicable to 12 and out of the 12 that is applicable the city's ICT governance Framework is found to be compliant to 11 making the city 92% compliant with POPIA conditions.

3.9 Conclusion

This chapter explained the content analysis process in which three TFFM documents (Buyers Registration SOP, License Agreement and Service Level Agreement) were analysed. In addition, the CoT's IT governance framework was also analysed. Of the three personal information processing and handling documents that TFFM use, one has scored 80% for the POPIA compliance test whilst the other two scored below 50%. The CoT's IT Governance framework document scored 92% for the POPIA compliance test which reveals that

there is a compliance gap between the TFPM and CoT. Thus it was observed that the CoT has put in place a framework to ensure compliance, whereas the TFPM has not made considerations to this framework when formulating their own operational procedure relating to the handling of personal information. Although the study does not aim to address the CoT's non-compliance, the 8% non-compliance on CoT's IT governance framework is triggered by only one missing important aspect that being the non-presence with the POPIA compliance framework as reflected on the compliance checklist in Table 3.4. The CoT should in addition, develop a POPIA compliance framework which must be cascaded down to all divisions dealing with personal information within the city including the theTFPM. Moreover, the TFPM should ensure the alignment of the three evaluated documentation (Buyers Registration, License Agreement and Service Level Agreement) to CoT's IT governance framework. To close the 55%, 70% and 20% gaps of non-compliance on the analysed documents, the TFPM should develop a POPIA compliance framework that is compatible to the business operations of the market.

Chapter 4

Research Methodology

4.1 Introduction

Chapter 3 discussed the process and findings of a content analysis of SOPs, SLAs, and the IT governance framework of the Tshwane Fresh Produce Market (TFPM) and the City of Tshwane (CoT) respectively. As observed in the conclusion of Chapter 3, a low rate of compliance with the POPIA was detected in the analysed documents. Furthermore, it was also detected that an alignment gap existed between the TFPM and the CoT's IT governance framework. The alignment and non-compliance gaps confirm the reports of challenges with POPIA compliance, from literature, as discussed in Chapter 2. This further indicates the need for a POPIA compliance framework within the TFPM. The objective of this chapter is to offer a detailed account of the rigorous methodology employed in developing a POPIA compliance framework for the TFPM. In this chapter, the research paradigm of the study, the research methodology and the research methods that were employed are discussed.

4.2 Research Paradigm

There are two major research paradigms in the academic sphere, namely qualitative and quantitative research. Quantitative research is associated with natural sciences, while qualitative research is widely associated with social sciences (Khaldi, 2017). Creswell (2003) defines quantitative research as a means for testing objective theories by examining the relationship among

variables. These variables in turn, can typically be measured on instruments so that numbered data can be analysed using statistical procedures. The author further defines a qualitative paradigm as a means for exploring and understanding the meaning individuals or groups ascribe to a social or human problem. Khaldi (2017), emphasizes that it is important that researchers in the academic sphere grasp an understanding of research paradigms as they determine the choice a researcher must make at all phases of their research process which invariably include the following:

- Research methodology choice
- Selection of the appropriate research tools for the collection of the data
- Procedure(s) followed for analysis and
- The nature of the conclusions they draw in their study

This study sought to understand and influence the personal information handling conduct of the TFPM and therefore subscribes to the qualitative research paradigm. As such, a methodology from the qualitative research paradigm was followed.

4.3 Methodology

Kothari (2004) describes research methodology as the process consisting of problem enunciation, hypothesis formulation, data collection and analysis with the aim of reaching a certain conclusion about the problem of concern or theoretical formulation. This study covers the aspects described by Kothari (2004) in the above paragraph by developing a POPIA compliance framework framework using the design science methodology. Delpont and Von Solms (Delpont & Solms, 2018), best describe design science methodology as a body of knowledge about the design of artificial objects and phenomena, artefacts, designed to meet certain desired goals. There are several approaches a researcher may embark on when undertaking a design science research study and these approaches are the Peffers approach, Design-Oriented Information System (Design-Oriented IS) approach and Design-Based approach (Delpont & Solms, 2018). For this study, the combination of Design- Oriented (IS) and

Research-Based approach as a customised methodology used by Nelson Mandela University for research about development of frameworks and strategies will be applied to develop a POPIA compliance framework. The methodology is categorized into four stages (Analysis, Design, Evaluate, Diffuse) which the researcher explored in their orderly fashion.

4.3.1 Analysis Stage

Analysis is the initial stage of the NMUDSFM, whereby the problem areas with regard to POPIA within the city of Tshwane were investigated in detail, thus scaling down to the exact problem which the study aims to resolve. After having transparently displayed the problem, the phase highlights the primary and secondary objectives which guide the entire treatise development process. To address the problem statement outlined in the introduction chapter, a literature review was undertaken to analyse and identify POPIA conditions. Further to the exploration of the problem area and highlighting study objectives, this phase also outlines in detail the conducted literature review to identify the subject area and other aspects of IT governance.

4.3.2 Design Stage

This stage entails a thorough review of the problem context to identify factors to be addressed by the solution identified in the analysis stage. The design stage was guided by factors identified during a literature review and used to conduct a content analysis of the TFPM SOPs and CoTs IT governance framework. The proposed solution is highlighted in this stage by developing an initial draft of the artifact (POPIA compliance framework) as described by the main objective of the study.

4.3.3 Evaluate Stage

The third stage of the NMUDSFM, entails refinement of the solution described in the design stage. Identification of participants for evaluation, data collection, data analysis and the implementation of proposed interventions were performed within this phase, which were repeated until the satisfactory result for all stakeholders was achieved. Semi-structured interviews with

members of the executive management of the TFPM were used to evaluate a draft of the developed POPIA compliance framework.

4.3.4 Diffuse Stage

This is the final stage of the methodology process, where a final compliance framework is realized. The final framework is further evaluated to ensure adherence to the NMUDSFM design principles. Additionally, the findings of the study are presented to the relevant audiences.

4.4 Research Methods

A research method is a mechanism used to collect and analyse data in pursuit of the main and sub-objectives of the study and describes the unfolding model that occurs in a natural setting that enables the researcher to develop a level of detail with high involvement in the actual experiences (Williams, 2007). In this study, the literature review, content analysis, modelling, expert interviews and logical argumentation were applied. The application of these research methods is discussed in sections 4.4.1 through 4.4.3.

4.4.1 Literature Review

A literature review is a means of demonstrating knowledge and consideration of the field of research by reading and presenting an overview of published works on a specific topic. A researcher cannot produce a significant study without first understating the literature review in their field. Through a literature review, the researcher displays knowledge depth, key variable, vocabulary, and history about the area of study (Randolph, 2009). In this study, the researcher achieved sub-objective 1, by identifying the conditions for lawful personal information processing as outlined in the POPIA. The findings of the literature review were then used in the development of a content analysis to investigate the personal information processing conduct of the TFPM.

4.4.2 Content Analysis

Bryman (2011) defines the content analysis process as a methodology that analyses documents, transcripts, interviews, text, audio, and video content in a detailed construed manner. In the context of this study, content analysis methodology was employed to analyse the IT framework of the CoT and the Service Level Agreements (SLAs), as well as the Standard Operating Procedures (SOPs) used by the TFPM in operations involving collection and handling of personal information. With the content analysis process the researcher investigated the personal information conduct of the TFPM and its alignment to POPIA conditions as outlined by sub-objective 2 of the study. From the discoveries of the content analysis, the researcher constructed a matrix/compliance test of the findings of the content analysis. This matrix assisted the researcher in measuring the level of compliance with POPIA conditions by the TFPM. The outcomes of the content analysis revealed that there is a compliance gap between TFPM SOPs and CoT's IT governance framework. While the CoT's IT governance framework displayed compliance with a considerable number of POPIA conditions, there was a low level of compliance with the SOPs and the SLAs of the TFPM. The outcomes of the compliance levels are outlined in Chapter 3 of this study.

4.4.3 Expert Review

Leedy and Ormrod (2001) define the semi-structured interview as the phenomenological approach to understanding an experience from the participants point of view. The authors further describe this method as the procedural format assisted by open-ended questions that explore the meaning of the experience in the subject study. Conducting the semi-structured interviews, analysing the data to find the clusters of meanings, and ending with a report that furthers the readers understanding of the essential structure of the experience (Creswell, 2003). The final research method for this study is expert review/interviews with the executive management of TFPM to validate the developed framework in line with the POPIA conditions. Expert review methodology is used to ascertain subjective responses from experts about a particular phenomenon they might have experience and their observations on practices relating to handling of personal information (McIntosh

& Morse, 2015). Prior to the actual semi-structured interview, the researcher performed a brief presentation of the conceptual framework to the participant which followed by a set of semi-structured interview questions shared via an email to the participant. The participants were asked to have their responses typed on the provided questionnaire to capture a detailed response. These responses were analysed using the affinity diagram tool. Crossman (2020) defines purposive sampling as a non-probability method selected based on characteristics of a population and the objective of the study. The study used the purposive sampling method for the purpose of selecting respondents as expert reviewers of the developed framework. The City of Tshwane's department of Economic Development and Spatial Planning has a number of senior managers who are heavily involved in development of policies and standard operating procedures both at strategic and tactical levels who as per the objectives of this study were the population of this study given their characteristics and experience in the organisation. During the expert review process, three of the senior managers were selected as participants for this study. Vasileiou, Barnett and Thorpe (2018) state that qualitative research does not have a straightforward answer to the question of 'how many' and that sample size is contingent on several factors relating to epistemological, methodological, and practical issues. The authors further emphasize that samples in qualitative research tend to be small to support the depth of case-oriented analysis that is fundamental and that samples are purposive, that is, selected by virtue of their capacity to provide richly textured information, relevant to the phenomenon under investigation. On this premises, the depth of knowledge and insights from at least one of the experts was sufficient, although inputs from all three are desirable.

4.5 Conclusion

The main aim of this chapter was to describe the methodology that guided this study. The methodology makes it scientific and therefore reproducible with the same or similar results. The problem statement and the objectives of the study were revisited to reaffirm alignment with the primary objective of the study. The chapter further highlighted the various research paradigms as described by literature and identified the qualitative paradigm as the suitable

approach for this study. Further to the research paradigm, the chapter briefly described the research methodology used for this study as prescribed by the Nelson Mandela University. The design-science research methodology was described in alignment with the Nelson Mandela University Design Science Framework (NMUDSF), a methodology used by Nelson Mandela treatise developers to create artifacts. For achievement of the main objective of the study, three research methods were used and these methods were clearly expressed in this chapter to provide a clear picture of the process of the study. The literature review, content analysis and semi-structured interview were comprehensively described based on literature in alignment with the 4 phases outlined by the NMUDSF methodology. The research paradigm, methodology and methods undertaken in this study enabled and simplified the development of the POPIA compliance framework process and realization of the primary objective of this study.

Chapter 5

Development of a Protection of Personal Information Act Compliance Framework

5.1 Introduction

Chapter 3 of this study has analysed the content of various governance documentations for both TFPM and CoT in depth. During the analysis process, the CoT's corporate governance framework and TFPM ICT governance were reflected and expressed. These frameworks were evaluated against the requirement of POPIA, and some compliance gaps were identified. This chapter is the core section of this study as it depicts the solution of the identified problem with an aim of achieving the primary objective of the study. The primary objective of the study was to develop a POPIA compliance framework for the TFPM and this chapter aims to achieve that. Chapter 2 of this study discussed literature about the existing frameworks available globally to assist personal information handling organisations to comply with personal information legislation as part of their IT governance efforts. Literature in South Africa and abroad was reviewed and the lack of literature for compliance frameworks was evident as there were limited personal information compliance frameworks and guidelines.

This chapter presents the solution of the study for the research problem defined in Chapter 1. This chapter discusses the construction of a proposed POPIA compliance framework for the TFPM. The discussion in this chap-

ter highlights and describes existing models that could be adapted to construct a POPIA compliance framework for the TFPM. The chapter begins by outlining and reflecting on TFPM's ideal governance structures that were developed by the researcher based on the current operating model of the market. Following the ideal governance model, the chapter further outlines the personal information collection and processing workflows while listing the type of personal information collected and processed by each entity on the reflected models.

5.2 Tshwane Fresh Produce Market Governance Levels

5.2.1 Strategic Level

Although the market is a division of the Department of Economic Development and Spatial Planning within the City of Tshwane, the strategies of the city are driven at the corporate level of the city as per the City's Governance Framework. The magnitude and the complexities of the market's operation dictates a strategic direction at its division level and therefore is "strategic" in the context of the above model. In the context of this study, the divisional head (Market Master) serves as a strategic leader of the market and together with his directors' (head of units) form a strategic body of this important entity.

5.2.2 Tactical Level

The tactical level is the administrative process of ensuring that the objectives set at the strategic level are implemented. In the context of TFPM this role is played by both the directors and functional managers (Functional Heads and Deputy Directors). This therefore means that directors/heads of units are active at both strategic and tactical levels.

5.2.3 Operational Level

The operational level consists of the functional administration of the daily market duties. These duties are performed by the market cashiers, trading

system administrators; other functions are performed for the market trading system by respective business operators of the market. The teams performing these duties are supervised by functional managers. It is the duty of the functional managers to ensure that policies and procedures are adhered to.

5.2.4 Office of the Divisional Head

As stated in the introduction chapter of this study according to the structures of CoT, TFPM is a division amongst other divisions that fall under the city's department of Economic Development and Spatial Planning. The office of the divisional is the top office of the market and the Divisional Head acts as the CEO of the market. In that sense the office of the Divisional Head is the highest office of the market. The primary role of this office is to set a strategic direction for the market at a divisional level taking accountability for activities in the market.

5.3 Personal Information Collection

As stated in the background for this study, the City of Tshwane's Fresh Produce Market (TFPM) is a division within the structure of the City's department of Economic Development and Spatial Planning. Its main function is to provide a fresh produce trading platform for its stakeholders in the form of building facilities, trading system, ICT infrastructure with its secondary function being an ombudsman for producers and buyers regarding the trading conduct of market agencies, by developing bylaws and ensuring adherence to them. In conducting its normal daily operations, the market collects personal information from agents, buyers, and producers as the critical stakeholders of the market.

5.3.1 Personal Information Collection Workflow and Stakeholders

The workflow below presents how personal information is handled between the collection point and the processing point by TFPM's internal stakeholders involved.

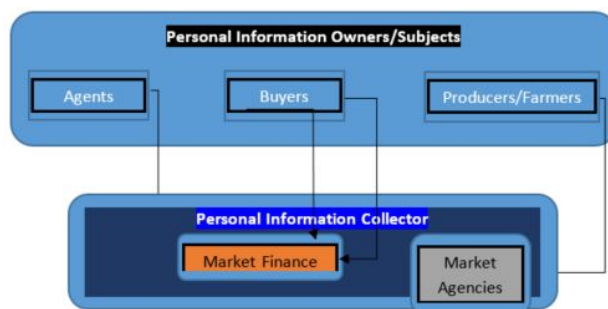


Figure 5.1: Personal Information Collection Workflow

In the context of the TFPM, collected and processed personal information in the main belong to the three owners namely:

- Market Agents
- Market Buyers
- Producer/Farmers

Each of the above are discussed in the sections that follow.

Market Agents

Market Agents are salespersons employed by market agencies to operate by sourcing farmers to bring produce to the market and to sell such produce on their behalf. Before an agent can be employed by an agency, personal information must be collected and recorded on the market trading system. Although the market plays a role in the recruitment process of such agents, the responsibility of collecting such personal information falls under the market agency and not the market. The market only becomes involved when the personal information is processed and maintained.

Market Buyers

Market buyers are buyers that purchase fresh produce on the market floors from various market agencies. These buyers range from big buyers to informal traders. Big buyers are those that buy for medium to large wholesalers and retailers while informal traders are mainly the street vendors and small shops. For one to become a buyer at the TFPM, a buyer registration process

must be followed whereby personal information is collected by the Market's Finance Department at the cashiering services. There are two types of buyers at the TFPM from whom personal information is collected, namely normal buyers and EFT (Electronic Funds transfer) buyers. Each of these buyers is provided with a buyer's tag on completion of their registration which serves as an account device for all transactions made by them.

Farmers/Producers

Farmers are the reason for the existence of the fresh produce markets around the world and without them the fresh produce market business is null and void. For a farmer to be able to supply their produce to the TFPM they need to be registered on the market trading system and during the registration process, some personal information is collected. The registration and collection of personal information at the first phase is conducted by the Agency as the recruiter of the producer.

Table 5.1: Types of Personal Information Collected

Agents	Buyers	EFT Buyers
Name	Name	Name
Surname	Surname	Surname
Contact Details	Contact Details	Contact Details
	Identity Number/copy	Identity Number/copy
	Residential Address	Residential Address
	Business Address	Business Address
		Banking Details
Personal Information Collector		
Market Agencies	Market Cashiering Services	Market Cashiering Services & Market Agencies

Table 5.1 depicts the categories of personal information collected by the TFPM from agents, buyers and producers. The table also shows the collectors of this personal information.

5.4 Personal Information Processing Workflow

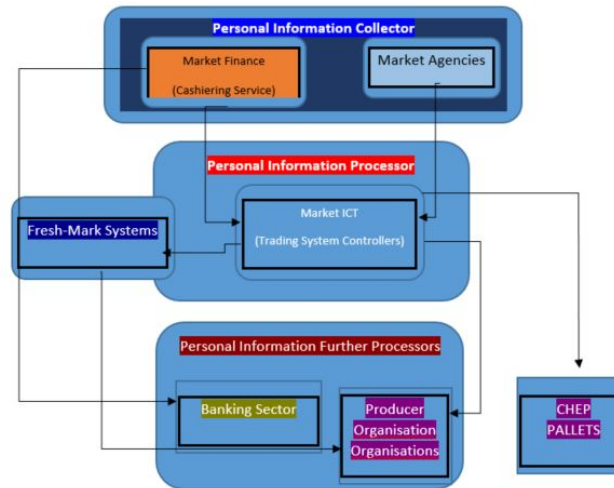


Figure 5.2: Personal Information Processing Workflow

As stated in Figure 5.1: Personal Information collection workflow, personal information is collected from three owners, namely: agents, Buyers and producers. This information is then captured on the Fresh-mark's refresh trading system for processing by trading system controllers working for the market under the market ICT section. As reflected in Figure 5.2, processing does not end with the market ICT but Fresh-Mark as the service provider has a processing role to play at the same level as the market ICT. This processing is in the main referred to Fresh-Mark by the market ICT trading system controllers for technical escalatory purposes. Processing does not end with the service provider. ABSA bank has been the banking partner of the market for over 30 years; various financial transactions take place through the Fresh-mark trading system which is integrated to relevant modules on the ABSA banking system. These financial transactions are performed by market officials and are mainly payments to producers and deposits by buyers.

Table 5.2: A Table of POPIA Responsibilities

No.	Governance Level	Role	Responsibilities
1.	Strategic	Divisional Head	<ul style="list-style-type: none"> • Appoint a POPIA Compliance Officer • Approve POPIA Compliance Framework • Ensure regulative and regulatory compliance • Approve POPIA required the policies • Ensure proper Risk Management
2.	Strategic	Directors	<ul style="list-style-type: none"> • Develop the POPIA compliance framework • Develop POPIA required policies • Develop POPIA processes and procedures • Ensure adherence to POPIA policies • Ensure adherence to POPIA processes and procedures • Risk Management
3.	Tactical	Directors & Deputy Directors	<ul style="list-style-type: none"> • Implement the POPIA compliance framework and policies. • Implement POPIA processes and procedures. • Provide training on POPIA compliance • Communicate to stakeholders about POPIA.
4.	Operational	Functional Administrators	<ul style="list-style-type: none"> • Adhere to POPIA policies • Adhere to POPIA processes and procedure on daily operations

5.4.1 POPIA Non-Compliance Risk and Impact

Table 5.3 below outlines possible major risks related to non-compliance with POPIA and the impact they might have on the TFPM. The table also highlights the relevant mitigation for respective identified risks.

Table 5.3: A Table of Risks from POPIA Non-Compliance

Risk Type	Impact	Mitigation
Reputation	Damage to the reputation of the TFPM and the CoT at large.	Appoint a Compliance Officer.
Non-Compliance	Fines by the Information Regulator and the arrest of the Accounting Officer.	Develop compliance procedures, policies and processes and ensure adherence to them.

5.5 Conceptual Framework

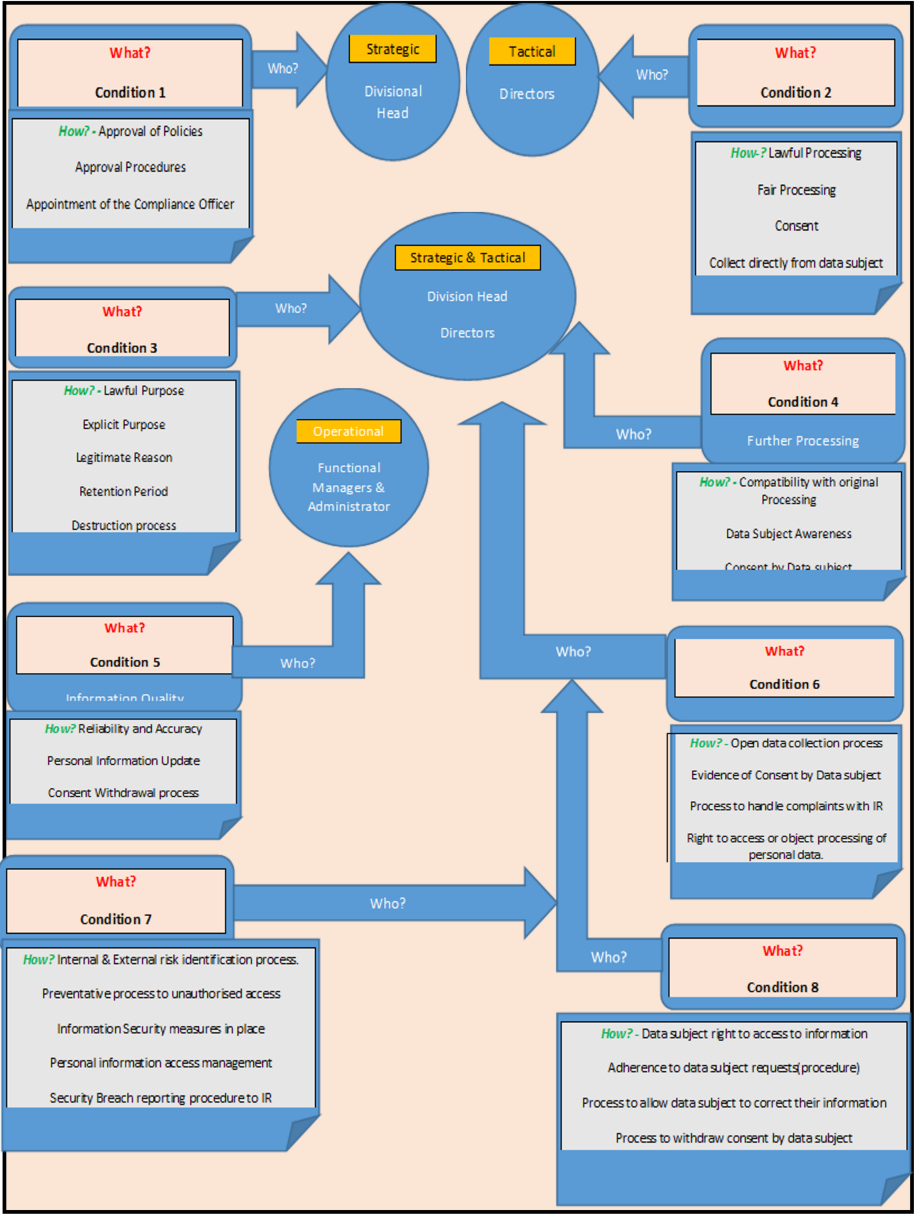


Figure 5.3: Conceptual POPIA Compliance Framework

Figure 5.3 reflects the proposed POPIA compliance framework that may be used to ensure safeguarding of the integrity and sensitivity of private information. The tool was developed based on the requirements stipulated in the legislation’s Chapter 3 about the conditions of POPIA as well as the IT governance structures within the CoT and TFPM.

Table 5.4: A Table of the Conceptual Framework Processes

Level	Who	What	How
1. Strategic	Divisional Head	Condition 1: Accountability	<ul style="list-style-type: none"> • Approval of policies • Approval of procedures • Appointment of the Compliance Officer
2. Tactical	Directors	Condition 2: Processing Limitation	<ul style="list-style-type: none"> • Lawful processing policies and procedures • Fair processing policies and procedures • Consent
3. Strategic/ Tactical	Divisional Head / Directors	Condition 3: Purpose Specification	<ul style="list-style-type: none"> • Lawful processing • Explicit purpose • Legitimate reason • Retention period • Destruction process
4. Strategic/ Tactical	Divisional Head/Directors	Condition 4: Further Processing Limitation	<ul style="list-style-type: none"> • Compatibility with original processing • Data subject awareness • Consent by data subject
5. Operational	Functional Managers & Administrative Personnel	Condition 5: Information Quality	<ul style="list-style-type: none"> • Reliability and accuracy • Personal information update • Consent withdrawal process

6. Strategic/ Tactical & Operational	Divisional Head/Directors, Functional Managers & Administrative Personnel	Condition 6: Openness	<ul style="list-style-type: none"> • Open data collection process • Evidence of consent by data subject • Process to handle complaints with IR • Right to access or object processing of personal data
7. Strategic/ Tactical	Divisional Head/Directors	Condition 7: Security Safeguard	<ul style="list-style-type: none"> • Internal & external risk identification process • Preventative process to unauthorised access • Information security measures in place • Personal information access management • Security breach reporting procedure to IR
8. Strategic/ Tactical	Divisional Head/Directors	Condition 8: Data Subject Participation	<ul style="list-style-type: none"> • Data subject right to access information • Adherence to data subject requests (procedure) • Process to allow data subject to correct their information • Process to withdraw consent by data subject

It is vital that there is a structured way of handling personal information

in the organisation to achieve the requirements outlined in every condition stated in Chapter 3 of POPIA. The above conceptual framework table aims to simplify the conceptual framework diagram presented in Figure 7. The table reflects who, how and what about the activities on collecting, processing, and storing of personal information in an attempt to ensure significant compliance with POPIA.

5.5.1 Accountability

Conditions 1 of the 8 conditions in the above conceptual framework table reflect the level of accountability, who is accountable, how to ensure accountability and what; applicable conditions in the context of the TFPM are outlined. This condition should be practiced and ensured at the strategic level by the divisional head of the TFPM through appointment of the POPIA Compliance Officer who will ensure that everything in relation to protection of information is done in line with the conceptual framework and the guidelines prescribed by the information regulator. Further to the appointment of the POPIA Compliance Officer, the divisional head in his duties for accountability should approve POPI (Protection of Personal Information) policies and procedures in line with this legislation (The Presidency, 2013, p. 23).

5.5.2 Processing Limitations

Processing Limitations are conditions 2 of the 8 conditions which are performed at a tactical level by directors of relevant business units within the TFPM. As stated in condition 1, the 'what' is represented by the name of the condition which in this case is Processing Limitation. On the 'how', the condition stipulates limitations about processing personal information in ensuring that it is collected in a fair and lawful manner and only with the consent from the data subject. To ensure that the above point is achieved, directors should develop policies and procedures that are emphatic on the fact that personal information should only be collected directly from the data subject and that they are aware that their information is being collected and consent to its usage. Directors should also clearly state in the policies and procedures that in cases of personal information being obtained from third

parties, a full consent from the data subject allowing sharing of their personal information is in place (The Presidency, 2013, p. 24).

5.5.3 Purpose Specification

Purpose specification outlines condition 3 of the 8 conditions and is performed at both strategic and tactical level by the divisional head and directors of relevant business units in the context of the TFPM. In addressing 'the how', relevant directors in the development of the policies and procedures should be emphatic on the point of personal information being collected for a specific purpose in an explicit and lawful manner. The purpose of collection needs to be specific, documented, and adhered to. The data subject has the right to know what information of theirs the organisation holds and for what purpose it was collected, the policies and procedures should ensure that this aspect is covered in linking the purpose of collection to a legitimate reason. The policies and procedures should further stipulate the time and period that this information can be retained by the TFPM and ensure its destruction after the stipulated retainment period. The divisional head must account for the personal information in place and the information that should be destroyed and the dates when this must take place. A procedure to keep track of the information that must be destroyed is key for this aspect (The Presidency, 2013, p. 26).

5.5.4 Further Processing Limitation

Condition 4 of the 8 conditions presents the elements of further processing limitation. This condition states that personal information may not be processed for a purpose outside what it was initially collected for unless there is compatibility with the original purpose. This condition is again both tactical and strategic and is pinned to both the divisional head and the relevant directors. In developing policies and procedures, directors should always bear in mind that reuse of personal information must always be in accordance and be compatible with the purpose for which it was collected. The procedures must also ensure that the data subject is informed and made aware that their personal information is being reused for the purpose in line with the original intent of collection. A consent by the data subject is vital in this case (The

Presidency, 2013, p. 28).

5.5.5 Information Quality

Information quality is the 5th condition of the 8 conditions. The condition states that the TFPM as the personal information collector, must take reasonable steps in ensuring that complete, accurate, not misleading and updated personal information is collected. This condition is performed at an operational level by the functional heads and administrative personnel in the context of the TFPM. Procedure developed by directors should clearly outline processes that will always ensure reliability and accuracy of personal information. It is the duty of the operational personal to ensure that they adhere to these processes and procedures for capturing reliable and accurate data. Validation mechanisms should be in place during capturing of personal information. This can be achieved through proper validation programmes on the IT systems that are used to collect personal information in the market. To adhere to this condition, processes should be in place to allow data subjects to update their own information or withdraw their consent. Although processes to align with the above point are developed at a tactical level, it is the responsibility of the operational staff to adhere and to guide the data subjects accordingly (The Presidency, 2013, p. 30).

5.5.6 Openness

Openness is a condition that is aligned with conditions 2 and 3 of the 8 conditions. The condition is again emphatic on the fact that the data subject must always be aware that their information is being collected and for what purpose is this information. Openness is one condition that requires the attention of the entire divisional structure of the TFPM. The divisional head, directors and the operational personnel all have a role to play regarding openness. The directors must ensure that there are processes in place to get consent from the data subject and that consent process is adhered to by the operational staff during collection of personal information. A consent form completed by the data subject might be a useful tool in this case as part of the personal information collection process. The process should further stipulate the purpose of collection to the data subject; this purpose too

might be reflected on the consent form as part of the process. As evidenced that the data subject has consented to collection and usage of their personal information, the consent form must be safeguarded as proof of consent. This process must also reflect the responsible person in the TFPM including their contact details. This process must be transparent on what procedure to follow should they need to lodge a complaint with the information regulator if they suspect any misuse of their personal information. It is the responsibility of the TFPM to advise the data subject of their right to report any suspected misuse to the information regulator and that must form part of the openness policy with respect to POPIA. Forming part of the openness, the data subject should clearly and openly be informed of the right to access their personal information or objection to its processing. Directors should ensure that a process addressing the above requirement is developed while the operational staff must adhere to such a process (The Presidency, 2013, p. 30).

5.5.7 Security Safeguard

Security Safeguard is the 7th condition of the 8 and is the core of all conditions as it ensures that confidentiality and integrity of personal information are maintained. The condition ensures that personal information is securely processed by putting in place appropriate organisational and technical measures in minimizing the risk of loss, unlawful access, modification, unauthorised disclosure and destruction of personal information. This condition again becomes the responsibility of personal information handlers at all levels within the TFPM. To achieve the above points, the TFPM should have procedures in place to identify any foreseeable internal and external risk to personal information. This procedure can be embedded in the City of Tshwane's Information Security Policy Framework to be used by all divisions dealing with personal information. The safety and security policies must include the enforcement procedures and processes to ensure strict adherence to prevent personal information from landing in unauthorised hands. Included in the policies should be a process determining which employees have permission to access personal information and which information they have access to. The TFPM must put in place technical mechanisms to trigger alerts whenever personal information is being accessed without authority. Additional to the alert triggering process, the TFPM should put in place a

process to identify the source of personal information breach and a procedure to get such a breach neutralized so that its reoccurrence is prevented. Through the contractual agreement the TFPM has with external parties as outlined in Figure 6 about personal information process workflow, required security measures must be established and maintained. This should be clear and in the form of a written contract and it is the responsibility of the third party to report any possibility of personal information being accessed without authorization. Included in the policies and procedures should be a process to inform the data subject about any incident involving their information being accessed without authorization. The data subject must immediately, via email, or any other written means of communication be notified should there be any suspicion of data breach involving their personal information. Such a data breach must also be reported to the information regulator and the reporting process must be included in the POPIA compliance policies and procedures to be developed by directors of the TFPM (The Presidency, 2013, p. 32).

5.5.8 Data Subject Participation

This is the 8th and final condition which stipulates that the data subject has a right to request their personal information from where it is held and may ask that it be corrected or deleted. This condition is a tactical and strategic level responsibility in the context of the TFPM. Directors should be aware that there are procedures in place to advise the data subject about their rights regarding access to their personal information held by the TFPM. This procedure must include processes allowing the data subject to request their personal information from the TFPM without it being declined or having to pay a charge. The tactical manager must also ensure that the developed procedures are adhered to by operational personnel. Included in the policies and procedures should be a process to allow the data subject to withdraw their consent should they wish to do so at any stage (The Presidency, 2013, p. 36).

5.5.9 Stakeholder Engagement

As it is stated in Figure 5.2 about the information processing workflow, about 4 stakeholders are involved in processing of personal information that is collected by TFPM. This personal information belongs to TFPM's internal stakeholder in buyers, agents and farmers as presented in figure 4 above. The information is then flowed out of TFPM to about 3 external stakeholders in-namely, Chep, ABSA bank, various Producer Organisations and FreshMark. It then becomes vital that TFPM ensures that this information is processed lawfully as dictated by condition 1,3 and 4 presented in the conceptual framework (Figure 5.3) above. The conditions require that a consent be provided by the 3 internal stakeholders before being provided to external stakeholders for further processing. TFPM should through policy and procedure development in consultation with all stakeholder, ensure that reasons for further processing are lawful, explicit, compatible with original processing purpose and that the 3 personal information owners are made aware of this further processing.

5.5.10 Conclusion

The main aim of this chapter was to develop the POPIA compliance framework to achieve the main objective of the study. In the process of developing the framework, the chapter explored the compliance requirements in relation to POPIA conditions. In conclusion the chapter addressed the main objective of this study by developing a POPIA compliance framework for the TFPM. Its efficacy will be evaluated by experts and used also to evaluate the TFPM's privacy policy as discussed in Chapter 6.

Chapter 6

Validation of the TFPM POPIA Compliance Framework

6.1 Introduction

A comprehensive presentation on the IT Governance structure of the TFPM and the workflow on how personal data is handled were done in Chapter 5 providing a clear view on the flow of personal informal within the TFPM. to the reader. This chapter reports on the expert interviews that was were conducted with 3three senior managers in the City of Tshwane's Economic Development and Spatial Planning (ED&SP) Department, to evaluate the efficacy of the developed POPIA compliance framework. The chapter begins with an explanation of the expert interview protocol that was followed to evaluate the framework. A discussion and analysis of responses follows, in a later section. Finally, changes made to the framework, resulting from the expert interview, are presented before the chapter is concluded.

6.2 Expert Interview Process

As stipulated by Oesterle, Hawkins, Hill and Brady (2010) , any study involving development of an artefact should be taken through an evaluation process to ensure scientific rigor. As stated in Chapter 4 of this study, the evaluation was qualitatively conducted through an expert interview process. As cited in the previous chapter contextualizing expert interviews, Vasileiou et. al, et al. (2018) contextualizing expert interviews, states that qualitative research

does not have a straightforward answer to the question of how many and that sample size is contingent on with several factors relating to epistemological, methodological, and practical issues. The authors further emphasize that samples in qualitative research tend to be small to support the depth of case-oriented analysis that is fundamental and that samples are purposive, that is, selected by virtue of their capacity to provide richly textured information, relevant to the phenomenon under investigation. For the purposes of this study, individuals were defined as experts based on their experience in policy development, experience in the position of senior management and the expertise in developing organisational . The profile scope that was set for this process was that the individual should possess at least 6six years experience in policy development, be a senior manager and be involved in framework development within the Department of Economic Development and Spatial Planning (ED&SP) and TFPM. With a written authority from the gate keeper, participants were invited via email invited to participate in the study and were reminded that participation was voluntarily. In addition to the invitation, participants were requested to complete a consent form indicating their willingness to participate in the study. The purpose of the study and its objectives were also provided. Responses were solicited through a questionnaire, also distributed via email, which the participants could completed at their leisure. Accompanying the questionnaire were the study summary document, a voice over presentation of the study, the developed draft POPIA compliance framework, the TFPM's edited privacy policy to be evaluated using the draft compliance framework, Ethics letter and a consent form that was signed and returned electronically via email by participants to the gate keeper. It is to be noted that through the entire data collection processes, the identities of participants were kept anonymous as no personally identifiable information was collected. The participants were given two weeks from the 30 May 2022 to 15 June 2022 to provide feedback.

6.3 Findings of the Expert Interviews

In this section, the responses to the expert interview questionnaire will be discussed. The format of this section will follow the structure of the data collection tool/questionnaire. However, the discussion on the efficacy evalu-

ation is was presented before the analysis of the longer responses obtained from Section B of the questionnaire.

6.3.1 Section A: Demographic

To ensure that the responses received were from individuals deemed as experts for this study, a demographical section was included. Of the four participants who were contacted, three responded and the received responses received met the criteria and were eligible to be considered as experts in policy and framework development. Two of the participants have had more than 10 years of experience in policy development and have had held senior management positions for over 15 years and rated themselves as experts. The third participant had 8 to 10 years of experience in policy development and also met the two other criteria with more than 8 years of experience in policy development and over 15 years of experience in a top management position.

Table 6.1 below provides an overview of the participants' profiles as and their relevancy in evaluating the POPIA compliance framework.

Table 6.1: Expert Review Respondent Demographics

Participant No.	No. of Years Policy Development Experience	Organisational Rank	No. of Years of Management Experience	Level of Policy Framework Development Knowledge
1	10+	Senior Manager	15+	Expert
2	10+	Senior Manager	15+	Expert
3	8 to 10	Top Management	15+	Expert

6.4 Section C: Efficacy of the Framework

The objective of this section of the questionnaire was to evaluate the efficacy of the POPIA compliance framework for the TFPM. By obtaining the experienced opinion of the respondents regarding the framework, it was determined that the framework is was fit for use in the TFPM. In Section C of the questionnaire, Likert scales ranging from 1 to 5 were used to obtain

the expert opinion of the participants. According to the range of the scales, scales, the values were defined as 1 = Strongly Disagree, 2 = Disagree, 3 = Neutral, 4 = Agree, 5 = Strongly Agree. The efficacy was composed of four questions where that the participants had to respond to after having evaluated the framework itself by the interviewing the processes, procedures and roles defined in the framework in accordance with the operations and needs of the TFPM. Each of these questions is analysed below based on the participants responses.

Table 6.2: Framework Efficacy Evaluation Responses

Question	Participant 1	Participant 2	Participant 3
The framework is in line with the TFPM and CoT's governance structures.	Agree	Strongly Agree	Strongly Agree
The framework will assist the TFPM to comply with POPIA.	Strongly Agree	Strongly Agree	Strongly Agree
The framework cover the significant requirements of the POPIA.	Strongly Agree	Strongly Agree	Strongly Agree
The framework is easy to understand and user friendly.	Strongly Agree	Strongly Agree	Strongly Agree

- Alignment of the framework with TFPM and CoT's Governance structures.** As observed in Table 14, participant number 1 agrees agreed that the framework aligns aligned with the TFPM and CoT's governance structures while participants number 2 and 3 supported by strongly agreeing with the question.
- Assistance of the framework to comply with POPIA.** On whether the developed framework would assist the TFPM to comply with the POPIA, all three participants strongly agreed that the framework would serve this purpose.
- Framework covering significant requirements of POPIA.** Question 3 which sought to determine if the framework is covered all significant requirements of POPIA it was noticed that all participants once again strongly agreed.

- **Framework User friendliness.** Fourth and finally, all three of the participants once again strongly agreed that the developed framework was easy to understand and made POPIA compliance user friendly.

6.5 Section B: Alignment of Practice with the SOPs

The purpose of this section was to ascertain that the information processing conduct of the TFPM was in alignment with the findings from the desktop research/content analysis conducted in Chapter 3 of this study. Affinity diagrams were used to analyse the responses and determine the gaps between the findings and the reported practice as obtained from the questionnaire respondents.

6.6 Analysis of Open-ended Responses

Affinity diagram is a popular analysis method used by groups for visualization and brainstorming of ideas by grouping them together. Among other modern methods of conducting an affinity diagram process, it is in the main undergone using sticky -note papers or white boards for simplicity and visibility (Widjaja & Takahashi, 2016). Kent (2016), supports utilization of the affinity diagram method simply because it allows opinions, complex data, and chaotic verbal data to be collected and organised in a manner that reveals basic actions that need to be taken. In many instances these data was collected through interviews and elaborative surveys/questionnaires.

This chapter uses the affinity diagram for analysis of the collected data participants. Affinity diagram is described by Plain (2007), as a qualitative analysis tool that presents a convenient tool to group and categorizes seemingly dissimilar data. During this process, the large amount of collected disorganised data is grouped based on natural relationships using a creative process and not a logical process (Kiran, 2016). This data helps the analyst to arrive at a certain consensus. The method involves four critical steps where data is segmented and filtered to reach a certain conclusion. The four steps outlined in the affinity diagram method are as follows:

- **Generate affinity ideas** This step involves diagramming and evaluation of the initially collected data by basically copying and pasting verbatim responses from participants onto a created template.
- **Get ideas displayed** This step involves sticking all notes onto a wall but does not necessarily mean sticking on physical walls and as the process can be done electronically by creating tables with rows and columns where the collected data is pasted. In this chapter, this process was done by copying data from the response sheet onto an Excel spreadsheet.
- **Group ideas by sorting** This step involves walking through the wall reading all responses gathered to identify similarities and pasting relevant information.
- **Analysis of Findings** This step was undergone by analysing each question based on the responses from each participant.

Table 6.3, below outlines responses provided by expert interviewers 1-3. The feedback has been copied and pasted as is from the questionnaire that the interviewer used to elicit responses from the experts.

Table 6.3: Discussion Question Responses

Question	Participant 1	Participant 2	Participant 3
Does the company take all reasonable steps to prevent personal information being lost or damaged or unlawfully accessed and modified?	Yes. Personal information is kept within dedicated areas accessed only by specific users. There are physical and logical access controls in place where access to such information is managed.	Yes. The act compels any organisation or any person who keeps any type of records relating to the personal information.	Yes. Access to producers' and buyers' information is restricted to certain individuals within the company.
Is the purpose of the collection and processing of the personal information clearly set out and defined in company processes?	No. Personal information is only collected for the purpose that is relevant to such collection.	Yes. The standard operating procedures to deal with personal information are clearly outlined.	No. It is not reduced to writing in a form of a policy. It is assumed that the purpose of the collection and processing of the personal information is "generally known in the company".
Does your company process personal information in an adequate, relevant, and non-excessive manner, given the purpose it is processed for?	Yes. Personal information is only collected for the purpose that is relevant to such collection.	Yes. Human Resource's key accounts specialized are trained to process the information as per company procedures and process	Yes. Personal information is populated in a structured format in accordance with the company's requirements for use in for trading purposes and planning

Is the personal information of individuals available and easily accessible by relevant role-players within the company?	Yes. The information is only available to such role-players assigned to the process for which the information was supplied.	No. The personal information is not easily accessible but is available on request with motivation.	No. Relevant role players in the company have easy access to information. This was arranged this way to make it possible for them to perform their roles effectively.
Will the company 'further process' the personal information?	No. The information is only processed for the purpose that it was obtained for.	Yes. The personal information will be processed as per company Standard Operating Procedure.	Yes. Part of collected information is used in business operations and for strategy planning purposes.
Is the personal information of individuals available and easily accessible by relevant role-players within the company?	Yes. The information is only available to such role-players assigned to the process for which the information was supplied.	No. The personal information is not easily accessible but is available on request with motivation.	No. Relevant role players in the company have easy access to information. This was arranged as this way to make it possible for them to perform their roles effectively.
Does the company empower employees through training to work responsibly with personal information?	No. No substantiation	Yes. Human Resource Management conduct training for staff that are responsible to deal with personal information.	No. There is no training that I am aware of that is specifically meant to capacitate employees to work responsibly with personal information.
Has the company considered protection of the integrity and quality of the personal information?	Yes. Personal information is not divulged to third parties or persons who do not use such information for the purpose that it was acquired for. Consideration is also being given to ensuring the quality thereof by giving the buyer access to interview and update such information.	Yes. No substantiation.	Yes. The company restricts access to information and only certain employees have access to it.

Has the company appointed an Information Officer (IO) and is the IO's appointment registered with the Information Regulator?	Yes. The City of Tshwane has an information officer. The Tshwane Market falls within the ambit of such officer.	No. The appointment will be considered.	No. The company has appointed the Head of Market IT and it was not mandatory for him to be registered with the Information Regulator when his appointment was considered.
Does the company have a POPIA Compliance Framework?	Yes. The City of Tshwane has a POPIA compliance framework. The Tshwane Market must function within the framework.	Yes. It is mandatory to have POPIA compliance Framework	No. The Company plan to have it developed and implemented in the near future.
Is there a process individuals can follow to request details of the personal information held by the company?	Yes. The City of Tshwane's process must be followed.	Yes. SOP have been developed	No. Individuals in need of someone's personal information is required to make a request in writing to the Head of the market.
Does the company have a Retention of Records Policy, or a Retention Schedule incorporated in the Data Retention Policy?	Yes. The National Archives guidelines are followed.	Yes. The policy is available and well implemented.	No. The company does not have these policies but retains electronic trade data in servers on a regular basis.
Will the company transfer personal information over borders?	No. No substantiation	Yes. On request and per POPIA.	No. There has never been a request to transfer data above borders and should such a request be received; it is highly unlikely that the company will accede to such a request.
Has the company's Information Governance Maturity been assessed?	No. No substantiation	No. Not yet assessed	No. The company does not have Information Governance Maturity assessed.
Does the company have a Privacy Notice?	No. No substantiation	No. The privacy notice is still to be published.	No. No substantiation

Table 6.3, reflects how the participants responded in areas linked to the conduct of the TFPM in ensuring alignment between the findings in Chapter 3 (Content Analysis) and the actual conduct with the aim of identifying gaps that must be addressed in the revision of the developed framework.

6.6.1 Discussion of Findings

Question 1: Does the company take all reasonable steps to prevent personal information being lost or damaged or unlawfully accessed and modified?

For this question all participants agreed that the company is was taking all reasonable steps to prevent loss, damage, and unlawful accessing/modification of personal information. In the substantiation Participant 1 stated that personal information was kept within dedicated areas accessed by specific users and that physical and logical access controls were in place where access to such area was managed. Participant 2 just simply states stated that POPIA compelled any organisation or any person who kept any type of record for personal information without mentioning if the said organisation was doing what was required to safeguard personal information while Participant 3 simply stated that access to producers and buyers personal information was restricted to certain individuals within the company which is the statement that supported participant 1s response.

Question 2: Is the purpose of the collection and processing of the personal information clearly set out and defined in company processes?

Participant 1 did not agree with the fact that the purpose of collection and processing of data collection was clearly set and defined in the processes and policies of the TFPM. When substantiating this the participant simply states stated that although the purpose was not clearly set out, practically personal information was only collected for the purpose that was relevant to such a collection, while Participant 2 differed to Participant 1 by stating that standard operating procedures to deal with personal information were present and clearly outlined the purpose of collection and processing of personal information. Participant 2 stated that the purpose of collection and

processing was not reduced to writing in form of a policy, but the assumption was that the purpose of collection and processing of personal information was generally known in the TFPM. Participant 3, also conceded that the purpose of collection and processing of personal information was not clearly set out.

Question 3: Does your company process personal information in an adequate, relevant, and non-excessive manner, given the purpose it is processed for?

For this question all participants ticked ‘Yes’, agreeing that TFPM processed personal information in an adequate, relevant, and non-excessive manner and for the purpose it was collected for. When substantiating, Participant 1 mentioned that personal information was only collected for the purpose that was relevant to such a collection while Participant 2 stated that the Human Resource’s key accounts were specialised and trained to process the information as per the TFPM’s procedures and processes. Participants 3 simply stated that the personal information was populated in a structured format in accordance with the TFPM’s requirements for use in trading purposes and strategic planning.

Question 4: Is the individual whose personal information is collected and processed informed thereof?

Both participant 1 and 2 agreed that the individuals whose personal information was being collected and processed were informed along the process. Participant 1 substantiated that the individual completed the data collection forms that were relevant to the purpose thereof but did not clarify if these forms indeed informed the individuals for what purpose their personal information was being collected. Participant 2, in their substantiation stated that the disclaimer clearly mentioned the purpose for personal information collection and processing. Participant 3 supported Participant 2’s statement, by also stating that the disclaimer clearly mentioned the fact that personal information was confidential but responded ‘No’ to the question as opposed to Participants 1 and 2.

Question 5: Will the company further process the personal information?

On whether the TFPM would further process the personal information, Participant 1 denied by stating that personal information was only processed for the purpose that it was obtained for. Although the substantiation did not directly respond to the question, it was understood that because they chose 'No' as an answer, the participant said the TFPM did not further process the personal information of its clients. Although they agreed to the question by choosing, "Yes, Participant 2 just stated that personal information was processed as per the TFPM's standard operating procedure without directly responding to whether the information would be processed further or not. Participant 3 simply stated that the collected personal information was used for business operations and strategic planning purposes implying that this information was only processed internally within the TFPM and not taken outside the TFPM for further processing.

Question 6: Is the personal information of individuals available and easily accessible by relevant role-players within the company?

On accessibility of personal information by owners, Participant 1 agreed that available personal information was easily accessible by relevant role players within the TFPM and supported the statement by stating that information was available to such role players who were assigned to process it. Participants 1 and 2 disagreed with Participant 1, as they chose the 'No' option and further supported their choice by mentioning that personal information was not accessible but was available on request, with motivation. Although it was not clear from this response, the assumption was that there was a formal process in this regard and personal information processors were aware of such a process. Participant 3 also chose a 'No' option for this question substantiating that relevant role players within the TFPM had easy access to personal information and this arrangement was made to make it possible for responsible players to perform their role efficiently. This response reflects that personal information was easily accessible by officials within the TFPM but it is not clear in terms of the process in place for easy accessibility of personal information by owners.

Question 7: Does the company empower employees through training to work responsibly with personal information?

For the question of the employer empowering employees by training them to enhance their responsibility when working with personal information, Participant 1 responded with “No without providing any substantiation to the response. In contrast to participants 1 and 3, Participant 2 agreed that employees working with personal information were being empowered by training. In their substantiation they mentioned that Human resource Management conducted training for staff that were responsible to deal with personal information. In support of the participant, the 3rd participant also conceded that there was no training that they were aware of that was specifically meant to capacitate employees working with personal information.

Question 8: Has the company considered protection of the integrity and quality of the personal information?

For this question, all participants agreed that the TFPM considered protection of the integrity of the personal information with Participant 1 stating that personal information was not divulged to third parties or persons who did not use such information for the purpose that it was acquired for. The participant further mentioned that consideration was made to ensure the quality of information by providing buyers with access to interviews and updating this information. Although Participant 2 agreed with participant 1 and 3 in this regard, they did not substantiate their response. Participant 3 stated that the TFPM restricted access to personal information and only certain employees in the organisation had access to it.

Question 9: Has the company appointed an Information Officer (IO) and is the IOs appointment registered with the Information Regulator?

All 3 participants reflected a different view for the question of appointment of the information officer (IO). Participant 1 was of the view that the TFPM did not need to appoint an IO as the City of Tshwane had a Chief Information Officer who was registered with the information regulator and because the TFPM is a division in the city, this IO is accountable for the personal

information of the TFPM. Participant 2 had a different view in the sense that they did not see the TFPM as having an IO and mentioned that it was something that needed consideration while Participant 3 conceded that the TFPM did not appoint an IO but because there was a Head of Information Technology section, that could be regarded as the IO of the TFPM even though they were not registered with the information regulator.

Question 10: Does the company have a POPIA Compliance Framework?

Although they agreed that the TFPM had the POPIA compliance framework in place, participants 1 and 2 did not agree with Participant 1 and referred to the City of Tshwane's POPIA compliance framework that the TFPM must function with while Participant 2 stated that it was mandatory to have a POPIA compliance framework without making any reference to the TFPM or CoT having such a framework in place. Participant 3 displayed a completely different view by first disagreeing that there was a POPIA compliance framework in place and supporting their statement by stating that the TFPM planned to have a POPIA compliance framework developed soon.

Question 11: Is there a process individuals can follow to request details of the personal information held by the company?

Although they agreed that there was a process in place for individuals to request details of the personal information held by the TFPM, participant 1 and 2 made reference to two different processes. Participant 1 referred to the CoT's processes and proposes that the TFPM should comply to such, while Participant 2 referred to a Standard Operating Procedure that has been developed to address this question. Another interesting view was that Participant 3 conceded that there was no process in place that individuals could follow to request details of their personal information, but they could make requests in writing to the head of the TFPM should they require details of their personal information.

Question 12: Does the company have a Retention of Records Policy, or a Retention Schedule incorporated in the Data Retention Policy?

The participants displayed different responses/opinions to the question of TFPM having a retention policy or process in place. Participant 1 stated that the national archives guidelines were being followed, but they were not necessarily clear on whether the organisation had a retention policy in line with the national archives guidelines or the national archives guidelines that were used as the policy of the organisation. Participant 2 also agreed that there was a retention policy in place and supported their statement by stating that it was well implemented while Participant 3 disagreed with both participants 1 and 2 by conceding that the organisation did not have the policy or a process in place, but personal information was being electronically retained in servers on regular basis.

Question 13: Will the company transfer personal information over borders?

All the participants displayed different responses to the question of the TFPM transferring personal information across the borders of South Africa. Participant 1 responded with a 'No' without any substantiation or making any reference to a policy that supported their response. Although they also responded with a 'No', Participant 3 stated that there had never been a request to transfer personal data over borders of South Africa, but should such request arise it was unlikely that it would be allowed by the TFPM. Again, this participant did not refer to any policy or procedure that supported their response and statement. Participant 2 agreed that personal information was being transferred over the borders of South Africa, but only on request and guided by POPIA.

Question 14: Has the companys Information Governance Maturity been assessed?

For the question of the TFPM having its Information Governance Maturity (IGM) assessed, all 3 provided a 'No' with Participant 1 not substantiating their answer while Participant 2 stated that the IGM had not yet been as-

sessed. The 3rd participant stated that the TFPM did not have the IGM assessed.

Question 15: Does the company have a Privacy Notice?

Again, on the question of TFPM having a privacy notice, all participants responded with a 'No' with participants 1 and 3 not providing any substantiation and Participant 2 stating that the privacy notice was still to be published.

6.6.2 Content analysis findings compared to Expert Interview Findings

The below table displays a comparison between the outcome of the content analysis process that was conducted in Chapter 3 of this study with the responses provided by the expert interviewers in this chapter to identify areas of concurrence, and non- concurrence. In the context of this chapter, concurrence means that there were similarities between the participants' responses and findings made through analysis of the SOPs in Chapter 3 while non-concurrence reflects different responses on such.

Table 6.4: A Comparison of Content Analysis Findings with the Expert Interview Responses

Question	Content Analysis Finding	P. 1	P. 2	P. 3	Concurrence?
Does the company take all reasonable steps to prevent personal information being lost or damaged or unlawfully accessed and modified?	Y	Y	Y	Y	Y
Is the purpose of the collection and processing of the personal information clearly set out and defined in company processes?	Y	N	Y	N	N
Does your company process personal information in an adequate, relevant, and non-excessive manner, given the purpose it is processed for?	Y	Y	Y	Y	Y
Is the individual whose personal information is collected and processed informed thereof?	N	Y	Y	N	N
Will the company 'further process' the personal information?	N	N	Y	Y	N
Is the personal information of individuals available and easily accessible by relevant role-players within the company?	Y	Y	Y	N	Y
Does the company empower employees through training to work responsibly with personal information?	Y	N	Y	N	N
Has the company considered protection of the integrity and quality of the personal information?	Y	Y	Y	Y	Y
Has the company appointed an Information Officer (IO) and is the IO's appointment registered with the Information Regulator?	Y	Y	N	N	N
Does the company have a POPIA Compliance Framework?	N	Y	Y	N	N
Is there a process individuals can follow to request details of the personal information held by the company?	Y	Y	Y	N	Y
Does the company have a Retention of Records Policy, or a Retention Schedule incorporated in the Data Retention Policy?	Y	Y	Y	N	Y
Will the company transfer personal information over borders?	N	N	Y	N	N

Has the company's Information Governance Maturity been assessed?	N	N	N	N	Y
Does the company have a Privacy Notice?	N	N	N	N	Y

Studying the above comparison, the expert interview feedback is in concurrence with Chapter 3's content analysis feedback for eight areas, whereas there is non-concurrence on only seven areas. The responses in the above table reflect that the participants in most of the questions picked up the same shortfalls on the TFPM's compliance to POPIA requirements using the proposed framework and the area of non-concurrence. One or two participants responses are in line with the finding made in Chapter 3 which shows that the participants are not in agreement with regard to which the state of POPIA compliance within the TFPM. Given the above reflection, no revision of the framework will be done as all the participants expressed a high level of satisfaction on the framework as shown in Table 2: framework efficacy.

6.7 Conclusion

This chapter reported on the expert interviews that were conducted with three senior managers in the City of Tshwane's Economic Development and Spatial Planning (ED&SP) Department, to evaluate the efficacy of the developed POPIA compliance framework. A presentation of results based on the expert interview process was made using the affinity programme method. In the presentation responses from all participants were outlined for ease of comparison, followed by the framework efficacy table where scales of 1-5 were used to demonstrate the satisfactory level of all participants on the proposed framework with the result of a high level of satisfaction as all participants agreed and strongly agreed on all questions without any objections. Following this process, each response was independently analysed based on the participants answers for each question and the same was done also on the five outlined efficacy questions.

This chapter further compared the analysis of findings made in the chapter with responses from participants in this chapter. The comparison process focused on two elements being concurrence and non-concurrence for all

participants' responses and the findings of the content analysis in Chapter 3 using the Nexia questionnaire. The outcome of the comparison showed that the content analysis findings and the expert interview responses were in concurrence on nine instances, while there were seven instances of non-concurrence. Based on the outcome of the efficacy test reflected in Table 6.2 of this chapter and the concurrence comparison shown in Table 6.4, it was concluded that the efficacy of the framework was proven through the expert interview results (as in Table 3). Therefore, no further iterations of the framework or the expert interviews were conducted. The outcomes revealed by the framework assessment are supported by Purtova,(2018) as outlined in Chapter 2 that in the contemporary, hyper-connected world of data-driven environments there is a growing need for intensive compliance for protection of information.

Chapter 7

Conclusion and Recommendations

7.1 Introduction

This chapter concludes the study. It provides an overview and summary of findings by describing how the study process met the objectives presented in Chapter 1 of this study and how this study will contribute to the organisation and makes suggestions for any possible future results. Additional to presentation of how the study objectives were met, the chapter summarizes each chapter of the study. The chapter further provides recommendations on how the developed POPIA compliance framework may be utilized to improve the compliance status of the TFPM.

7.2 Research Summary

The section summarizes each chapter in this study and how it was conducted in alignment with the objectives.

7.2.1 Chapter 1

Chapter 1 introduces the study by providing a background on existing IT governance, regulative and regulatory frameworks used in South Africa and elsewhere in the world. These frameworks were described in detail on aspects related to theme of this study. A background on the origin of POPIA,

its requirements and possible consequences for non-compliance were further provided in this chapter. This chapter further described the TFPM, and how its handling of personal information is undertaken as the subject organisation for this study. The description of the TFPM was bundled with its relationship to its stakeholder regarding the collection, processing and storing of personal information. There is little guidance in South Africa in relation to the development and implementation of the POPIA compliance framework which puts the City of Tshwane and the TFPM at risk of not complying with the legislation that was identified as the problem statement for this study. The main objective with sub-objectives addressing the problem statement were also presented in this chapter. In conclusion of Chapter 1, a research process workflow in line with the Nelson Mandela University's Design Science Methodology Framework was presented as a guide on which process this study followed.

7.2.2 Chapter 2

The second sub-objective of the study was to identify requirements of POPIA that would impact the TFPM as the data handler, Chapter 2 embarked on a wide range of literature to identify such requirements. The literature review revealed the lack of a POPIA compliance framework in the context of South Africa. The chapter discovered that except for the guidelines issued by the information regulator (IR), not many organisations, industries, government bodies or professionals have developed a compliance framework in alignment with the protection of personal information act as required by legislation. A brief description of the GDRP used in Europe was made in this chapter which found that GDRP was more proactive than the framework in the US. Other information related legislations and regulations were presented in this chapter to identify similarities with POPIA requirements. The eight POPIA conditions were identified and described as the main requirements that impacted the TFPM as the handler of personal information.

7.2.3 Chapter 3

This chapter discussed the analysis for evaluation of the personal information documentation for both the TFPM and CoT using the NEXIA questionnaire.

Three TFPM documents (Buyers Registration SOP, License Agreement and Service Level Agreement) were evaluated while only one from CoT was evaluated. Of the three personal information processing and handling documents that the TFPM used, one scored 80% of the POPIA compliance test whilst the other two scored below 50%. The city's ICT Governance framework document scored 92% in the POPIA compliance test which revealed that there was a compliance gap between the TFPM and CoT. CoT has put in place various regulatory and regulative frameworks to ensure compliance, but the TFPM seems not to have considered this framework when formulating their own operational procedure relating to the handling of personal information. Although the study does not aim to address the CoT's non-compliance, the 8% non-compliance of CoT's IT governance framework was triggered by one missing important aspect being the non-presence of the POPIA compliance framework as reflected on the compliance checklist in Table 3.9 of this study. This chapter mainly addressed sub-objectives one of the study being to investigate the state of readiness of the TFPM in compliance with POPIA. It was found that there were several non-compliance gaps which had the potential of putting the TFPM at risk of contravening POPIA which results in heavy consequences.

7.2.4 Chapter 4

This chapter described the methodology that guided this study. The problem statement and the objectives of the study were revisited to reaffirm alignment with the primary objective of the study. The chapter further highlighted the various research paradigms as described by literature and identified the qualitative paradigm as the suitable approach for this study. Further to the research paradigm, the chapter briefly described the research methodology used for this study as prescribed by the Nelson Mandela University. The design-science research methodology was described in alignment with the Nelson Mandela University Design Science Framework (NMUDSF), a methodology used by Nelson Mandela treatise developers to create artifacts. To achieve the main objective of the study, three research methods were used and these methods were extensively discussed in this chapter to provide a clear picture of the process of the study. The literature review, content analysis and Expert Review/Interview were comprehensively described based on literature

in alignment with the four phases outlined by the NMUDSF methodology. The research paradigm, methodology and methods undertaken in this study enabled and simplified the development of the POPIA compliance framework process and realization of the primary objective of this study.

7.2.5 Chapter 5

The chapter was introduced by outlining the TFPM's corporate governance structure which describes responsibilities in relation to the development and implementation of policies and processes at strategic, tactical, and operational levels. This governance structure was included to reflect how POPIA related policies, processes and procedures and the compliance framework will be aligned in the context of the TFPM. The governance structure further simplified the process of developing a compliance framework as contextualization of the framework was drawn from this governance structure. The chapter further presented the personal information workflow within the TFPM and various stakeholders having a role in processing this personal information. In this chapter roles and responsibilities on collection, processing and storing of personal information at various governance levels have been outlined. To study the risk aspect linked to personal information, the chapter explored the GRC framework of the governance structure with the aim of identifying hidden aspects in relation to POPIA conditions and requirements. In conclusion the chapter addressed the main objective of this study by developing a POPIA compliance framework for the TFPM where its efficacy was evaluated by experts and used also to evaluate the TFPM's privacy policy in Chapter 6. The framework was comprehensively aligned to the eight conditions of POPIA to what, who and how each condition should be addressed in the developed a POPIA compliance framework.

7.2.6 Chapter 6

Chapter 6 reported on the expert interviews that were conducted with three senior managers in the City of Tshwane's Economic Development and Spatial Planning (ED&SP) Department, to evaluate the efficacy of the developed POPIA compliance framework. A presentation of results based on the expert interviews was made using the affinity programme method. In the presen-

tation responses from all participants were outlined for ease of comparison, followed by the framework efficacy table where scales of 1-5 were used to demonstrate the satisfactory level of all participants on the proposed framework, and as result a high level of satisfaction was achieved as all participants agreed or strongly agreed to all questions without any objections. Following this process, each response was independently analysed based on the answers of all participants for each question and the same was also done on the five outlined efficacy questions. This chapter further compared the analysis finding made in the chapter with responses from participants. The comparison mainly focused on two elements, namely concurrence and non-concurrence with all participant's responses and the findings of the content analysis in Chapter 3 using the Nexia questionnaire. The outcome of the comparison showed that content analysis and the responses were in agreement but did not agree on nine and seven instances respectively. Based on the outcome of the efficacy test reflected in Table 2 of this chapter and the compliance shown in the comparison Table 3, it was concluded that the revision of the proposed framework developed in Chapter 5 was not an option and therefore would be adopted on the first iteration. ?????

7.3 Review of Study Objectives

7.3.1 Sub-Objective 1

To identify requirements of POPIA that will impact the conduct of the Tshwane Fresh Produce Market as a data handler.

Sub-objective 1 of this study was to identify the requirements for POPIA compliance. This was achieved by the literature review. A literature review research method was used to investigate the handling of the personal information in compliance to personal information regulations and legislations and the presence of relevant frameworks. The European framework of personal information legislation was also looked at which was found to have some similarities with the proposed South African version. Except for the guidelines issued by the information regulator (IR), not many organisations, industries, government bodies or professional have developed a compliance framework in alignment with the protection of personal information act as

required by this legislation. These eight POPIA conditions were identified as the core requirements for any organisation that collects and processes personal information. The conditions were further expanded to provide detailed requirements under each condition and the repercussions of non-adherence. For this study, this sub-objective was achieved as the POPIA requirements together with other frameworks were successfully identified and explored in detail.

7.3.2 Sub-Objective 2

To analyse the data handling conduct of the Tshwane Fresh Produce Market in line with POPIA .

Sub-objective 2 of the study embarked on a process of evaluating the state of readiness of the TFPM with regard to POPIA given the current method of collecting and processing personal information. The objective was achieved through analysing documentation for both the TFPM and CoT. Three TFPM documents (Buyers Registration SOP, License Agreement and Service Level Agreement) were evaluated while only one from CoT was evaluated. Of the three personal information processing and handling documents that the TFPM use, one scored 80% of the POPIA compliance test whilst the other two scored below 50%. The city's ICT Governance framework document scored 92% in the POPIA compliance test which revealed that there was a compliance gap between the TFPM and CoT. CoT has put various regulatory and regulative frameworks in place to ensure compliance, but the TFPM has not taken this framework into consideration when formulating their own operational procedure in relating to how personal information was handled. Although the study does not aim to address the CoT's non-compliance, the 8% non-compliance on CoT's IT governance framework is triggered by only one important missing aspect being the lack of the POPIA compliance framework as reflected on the compliance checklist in Table 3.9. This sub-objective was achieved as several governance documentation within the organisation were analysed and gaps calling for the development of the compliance frameworks were identified.

7.3.3 Sub-Objective 3

To address the POPIA conditions by constructing a POPIA compliance framework for the Tshwane Fresh Produce Market. As outlined in the previous chapters, this sub-objective was achieved using the expert review process. The responses were analysed using the affinity diagram method. This process was successfully conducted reflecting how the proposed compliance framework would be useful in an organisation such as the TFPM. Given the outcome of the expert reviews, the framework was accepted at first draft and there was no requirement to reiterate it and therefore there were no changes made to the first version of the framework as it successfully identified gaps between CoT and the TFPM's governance structure.

7.4 Recommendations

- CoT needs to develop a POPIA compliance framework which must be cascaded down to all divisions handling personal information within the city including the TFPM.
- In addition to the above recommendation, the TFPM needs to ensure the alignment of the three evaluated documents (Buyers Registration, License Agreement and Service Level Agreement) and any other policy, SOP or procedure to CoT's IT governance framework.
- To close the 55%, 70% and 20% gaps of non-compliance to the evaluated documents, the TFPM also needs to investigate developing a POPIA compliance framework that is compatible with the business operations of the market.
- CoT/TFPM must consider hiring a POPIA Information Officer.
- Using the developed framework, the TFPM must review all SOPs, policies, and procedures to ensure that all requirements of POPIA are addressed.

Given the responses provided by participants in chapter 6 and their analysis, it is important that the framework is not used just to tick the box. As advised by Job (2021), businesses and organisations should move away from treating

POPIA compliance as a regulation checkbox exercise but rather regard it as an opportunity to build resilience against possible unauthorised personal data accessibility.

References

- Abiodun, O. P., 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. 2.
- Anderson, D., Abiodun, O. P., & Christoffels, A. (2020). Information security at South African universities-implications for biomedical research. *International Data Privacy Law*, 10(2), 180–186.
- Ashley, C. (2019). *Understanding Purposive Sampling: An Overview of the Method and Its Applications*.
- Badshah, A., Ghani, A., Shamshirband, S., Aceto, G., & Pescapè, A. (2020). Performancebased servicelevel agreement in cloud computing to optimise penalties and revenue. *IET Communication*, 14(7), 1102–1112.
- Beck, A. (2017). *Update: South Africa Cyber Incidents*.
- Botha, W. (2021). *POPIA deadline looms large for healthcare practitioners*.
- Brotby, K. (2009). *Information Security Governance: A Practical Development and Implementation Approach* (Vol. 53 ed.). New Jersey: John Wiley & Sons, Inc.
- Bryman, A. (2011). Mission accomplished?: Research methods in the first five years of leadership. *Leadership*, 7(1), 73–83.
- Cheng, L., Liu, F., & Yao, D. (2017). Enterprise data breach: causes, challenges, prevention, and future directions. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, 7(5), 1211.

- ChePa, N., Bokolo, A. J., Rozi, Nor Haizan, R., & Masrah, A. A. (2015). A Review on Risk Mitigation of IT Governance. *Information Technology Journal*, 14(1), 1–9.
- Claessens, S., Kose, M. A., & Terrones, M. E. (2012). How do business and financial cycles interact? *Journal of International Economics*, 87(1), 178–190.
- Creswell, J. W., Plano Clark, V. L., Gutmann, M. L., & Hanson, W. E. (2003). An Expanded Typology for Classifying Mixed Methods Research Into Designs. In *Handbook of mixed methods in social and behavioral research* (Vol. 36, pp. 209–240). Lincoln: SAGE.
- Da Veiga, A., Vorster, R., Pilkington, C., & Abdullah, H. (2017). Compliance with the protection of personal information act and consumer privacy expectations: A comparison between the retail and medical aid industry. *2017 Information Security for South Africa - Proceedings of the 2017 ISSA Conference, 2018-Janua*, 16–23.
- De Haes, S., Van Grembergen, W., & Debreceeny, R. S. (2013). COBIT 5 and Enterprise Governance of Information Technology: Building Blocks and Research Opportunities. *Journal of Information Systems*, 27(1), 307–324.
- De Haes, S., Van Grembergen, W., Joshi, A., & Huygh, T. (2020). Enterprise Governance of Information Technology: Achieving Alignment and Value in Digital Organizations. *Springer Nature*, 15–74.
- Delpont, P., & Solms, R. von. (2018). *Methodological Guidelines for Design Science Research*. Port Elizabeth.
- DST SA. (2016). *Republic of South Africa PROMOTION OF ACCESS TO INFORMATION ACT , 2000 MANUAL AS REQUIRED BY SECTION 14 (2) OF THE PROMOTION* (No. 2).
- Dugmore, J., & Sharon, T. (2008). *ITIL® V3 and ISO/IEC 20000*.
- Eiselen, S. (2014). FIDDLING WITH THE ECT ACT ELECTRONIC SIGNATURES. *PER/PELJ*, 17(6).

- El Kharbili, M., Stein, S., Markovic, I., & Pulvermüller, E. (2008). Towards a framework for semantic business process compliance management. *CEUR Workshop Proceedings, 339*(January 2008), 1–15.
- Elo, S., & Kyngas, H. (2008). The qualitative content analysis process. *Journal of Advanced Nursing, 62*(1), 107–115.
- Ernst and Young. (2020). *Protection of Personal Information Act a new era of privacy for South Africa* (Tech. Rep.).
- Goeken, M., & Alter, S. (2008). IT governance frameworks as methods. *ICEIS 2008 - Proceedings of the 10th International Conference on Enterprise Information Systems, 2 ISAS*, 331–338.
- Grealy, P., Mngomezulu, N., Tembedza, W., & Blom, K. (2021). *POPIA codes of conduct, information officers and applications for exemption*.
- Hiller, J., McMullen, M. S., Chumney, W. M., & Baumer, D. L. (2011). Privacy and Security in the Implementation of Health Information Technology. *B.U. J. Sci. & Tech., 1*.
- Hsieh, H. F., & Shannon, S. E. (2005). Three approaches to qualitative content analysis. *Qualitative Health Research, 15*(9), 1277–1288.
- Huxley, K. (2020). Content analysis, quantitative. In *Content analysis, coding*. SAGE Research Methods.
- Jafta, Y., Leenen, L., & Chan, P. (2020). An ontology for the south african protection of personal information act. *European Conference on Information Warfare and Security, ECCWS, 2020-June*(July), 158–167.
- Job, A. (2021). *The POPIA opportunity*.
- Juiz, C., Colomo-Palacios, R., & Gómez, B. (2018). Cascading ISO/IEC 38500 based Balanced Score Cards to improve board accountability. *Procedia computer science, 417–424*.
- Kandeh, A. T., Botha, R. A., & Futchler, L. A. (2018). Enforcement of the Protection of Personal Information (POPI) Act: Perspective of data

- management professionals. *SA Journal of Information Management*, 20(1), 1–9.
- Kent, R. (2016). *Quality Management in Plastics Processing*. Elsevier.
- Khaldi, K. (2017). Quantitative, qualitative or mixed research: which research paradigm to use? *Journal of Educational and Social Research*, 7(2), 15–15.
- Kiran, D. R. (2016). *Total quality management: Key concepts and case studies*. Butterworth-Heinemann.
- Konstantina Vasileiou, Julie Barnett, Susan Thorpe, & Terry Young. (2018). Characterising and justifying sample size sufficiency in interview-based studies: systematic analysis of qualitative health research over a 15-year period. *BMC Medical Research Methodology*, 18(1), 1–18.
- Leedy, P., & Ormrod, J. E. (2010). *Practical Research: Planning and Design* (9 ed.). New York, NY: Pearson.
- Mabunda, S. (2021). Cybersecurity in South Africa: Towards Best Practices. In L. Belli (Ed.), *Cyberbrics*. Springer.
- Marx, A., Moolman, A., & Ngwenya, M. (2016). INFORMATION TECHNOLOGY GOVERNANCE DISCLOSURE COMPLIANCE OF JSE-LISTED COMPANIES. *INTERNATIONAL JOURNAL OF eBUSINESS AND eGOVERNMENT STUDIES*, 8(1), 57–70.
- McIntosh, M. J., & Morse, J. M. (2015). Situating and constructing diversity in semi-structured interviews. *Global Qualitative Nursing Research*, 2.
- Milo, D., & Dela, P. (2021). *Information Regulator publishes guidance note on applications for prior authorisation*.
- Mirobi, G., & Arockiam, L. (2015). Service level agreement in cloud computing: An overview. In *International conference on control, instrumentation, communication and computational technologies* (pp. 753–758). IEEE.

- Modiha, E. (2018). *Identifying the challenges to implement King IV in Chapter 9 and public sector*. Master of business administration, North-West University.
- Oesterle, S., David Hawkins, J., Hill, K., & Bailey, J. (2010). Men's and Women's Pathways to Adulthood and Their Adolescent Precursors. *Journal of Marriage and Family*, 1436–1453.
- Parliament, E., & Council of the European Union. (2016). *General Data Protection Regulation*. London.
- Plain, C. (2007). Build an Affinity for KJ Method. *Quality Progress*.
- Purtova, N. (2018). The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, 10(1), 40–81.
- Randolph, J. (2009). A guide to writing the dissertation literature review. *Practical Assessment, Research and Evaluation*, 14(13).
- Raodeo, V. (2012). It Strategy and Governance : Frameworks and Best. *International Journal of Research in Economics & Social Sciences*, 2(3), 49–59.
- Schwartz, P. M., & Peifer, K.-N. (2017). Transatlantic Data Privacy Law Permalink. *Georgetown Law Journal*, 106(1), 115–179.
- Staunton, C., Adams, R., Dove, E. S., Harriman, N., Horn, L., Labuschaigne, M., Mulder, N., Olckers, A., Pope, A., Ramsay, M., Swanepoel, C., Ni Loideain, N., & De Vries, J. (2019). Ethical and practical issues to consider in the governance of genomic and human research data and data sharing in South Africa: a meeting report. *AAS Open Research*, 2(May), 15.
- Team, C. (2022). *What is a Licensing Agreement?*
- The Presidency. (2013). *Protection of Personal Information Act 4 of 2013*.
- Widjaja, W., & Takahashi, M. (2016). Distributed interface for group affinity-diagram brainstorming. *Concurrent Engineering*, 24(4), 344–358.

Williams, C. (2007). Research Methods. *Journal of Business & Economics Research*, 5(3).

**PERMISSION TO SUBMIT FINAL COPIES
OF TREATISE/DISSERTATION/THESIS TO THE EXAMINATION OFFICE**

Please type or complete in black ink

FACULTY: Engineering Built Environment and Technology (EBET)

SCHOOL/DEPARTMENT: School of Information Technology

I, (surname and initials of supervisor) Prof M. Gerber

and (surname and initials of co-supervisor) T.H. Speckman

the supervisor and co-supervisor respectively for (surname and initials of

candidate) P.H. Malepeng

(student number) 223053511 a candidate for the (full description of qualification)

Master of Philosophy in Information Technology Governance

with a treatise/dissertation/thesis entitled (full title of treatise/dissertation/thesis):

A Protection of Personal Information Act Compliance Framework for the City of Tshwane's Fresh Produce Market

It is hereby certified that the proposed amendments to the treatise/dissertation/thesis have been effected and that **permission is granted to the candidate to submit** the final bound copies of his/her treatise/dissertation/thesis to the examination office.



SUPERVISOR

16 March 2023

DATE

And




CO-SUPERVISOR

16 March 2023

DATE

Signature Certificate

Reference number: DZXKX-X8TVB-TJZRB-5JON5

Signer	Timestamp	Signature
Pheah Malepeng Email: pheahm@tshwane.gov.za Sent: 17 Mar 2023 13:14:35 UTC Signed: 17 Mar 2023 13:14:35 UTC	17 Mar 2023 13:14:35 UTC 17 Mar 2023 13:14:35 UTC	

IP address: 198.54.1.102
Location: Pretoria, South Africa

Document completed by all parties on:
17 Mar 2023 13:14:35 UTC

Page 1 of 1



Signed with PandaDoc

PandaDoc is a document workflow and certified eSignature solution trusted by 40,000+ companies worldwide.

