A validated information privacy governance questionnaire to measure the perception of how effective privacy is governed in a financial institution in the South African context

By

PAULUS SWARTZ

Submitted in accordance with the requirements for

the degree of

MASTER OF SCIENCE

In the subject

INFORMATION SYSTEMS

at the

UNIVERSITY OF SOUTH AFRICA

Supervisor: Dr A. da Veiga

Co-Supervisor: Prof. N. Martins

April 2019

DECLARATION

Name : Paulus Swartz
Student number : 36278580
Degree : MSc in Computing

A validated information privacy governance questionnaire to measure the perception of how effective privacy is governed in a financial institution in the South African context

I declare that the above dissertation is my own work, and that all the sources that I have used or quoted have been indicated and acknowledged by means of complete references.

_____ 25 April 2019

SIGNATURE DATE

ACKNOWLEDGEMENTS

Firstly, I would like to thank our heavenly Father for His grace and strength that allowed me to complete this dissertation.

My heartfelt thanks and appreciation go to my supervisors, Dr A. da Veiga and Prof. N. Martins, for their support, guidance, invaluable advice and constructive comments during the study. I started the race and reached the finish line with your help.

A big thank you to my wife, my pillar, for your love and support, and for encouraging me to always go the extra mile. Thank you for your understanding and patience during my studies.

My two daughters, thank you for your unconditional love, support and patience while I was busy with my dissertation.

I would like to thank the following people who have helped to make the completion of this dissertation possible:

- The organisation for allowing me to conduct the survey and to use the data for my study. The managers and staff at the organisation for their participation and support: without you there could not have been a study.
- Dr E.C. Martins and Organisational Diagnostics for administering the survey.
- Dr L. Korf for her quick response and assistance in analysing and interpreting the data for the study.
- Ms. Y. Smuts for the professional language editing of my dissertation.
- My family for their love, support and encouragement.

ABSTRACT

The general aim of this research is to develop a conceptual privacy governance framework (CPGF) that can be used to develop a valid and reliable information privacy governance questionnaire (IPGQ) to assess the perception of employees of how effective the organisation governs privacy.

The CPGF was developed to incorporate a comprehensive set of privacy components that could assist management in governing privacy across an organisation. IPGQ statements were derived from the theory of the sub-components of CPGF, evaluated by an expert panel and pre-tested by a pilot group. A quantitative mono method research was followed using a survey questionnaire to collect data in a financial institution in South Africa. Exploratory Factor Analysis (EFA) was used to determine the underlying factorial structure and the Cronbach Alpha was used to establish the internal reliability of the factors. From the initial item reduction of the constructs, four factors were derived to test the privacy perception of employees. The IPGQ consisted of 49 valid and reliable questions. One-way Analysis of Variance (ANOVA) was used, and three significant differences were discovered among the demographical groups for the age groups and two for the employment status groups (organisational commitment and privacy controls).

The CPGF and IPGQ can aid organisations to determine if organisations are effectively governing the privacy in the organisations in order to assist them in meeting the accountability condition of the Protection of Personal Information Act (POPIA).

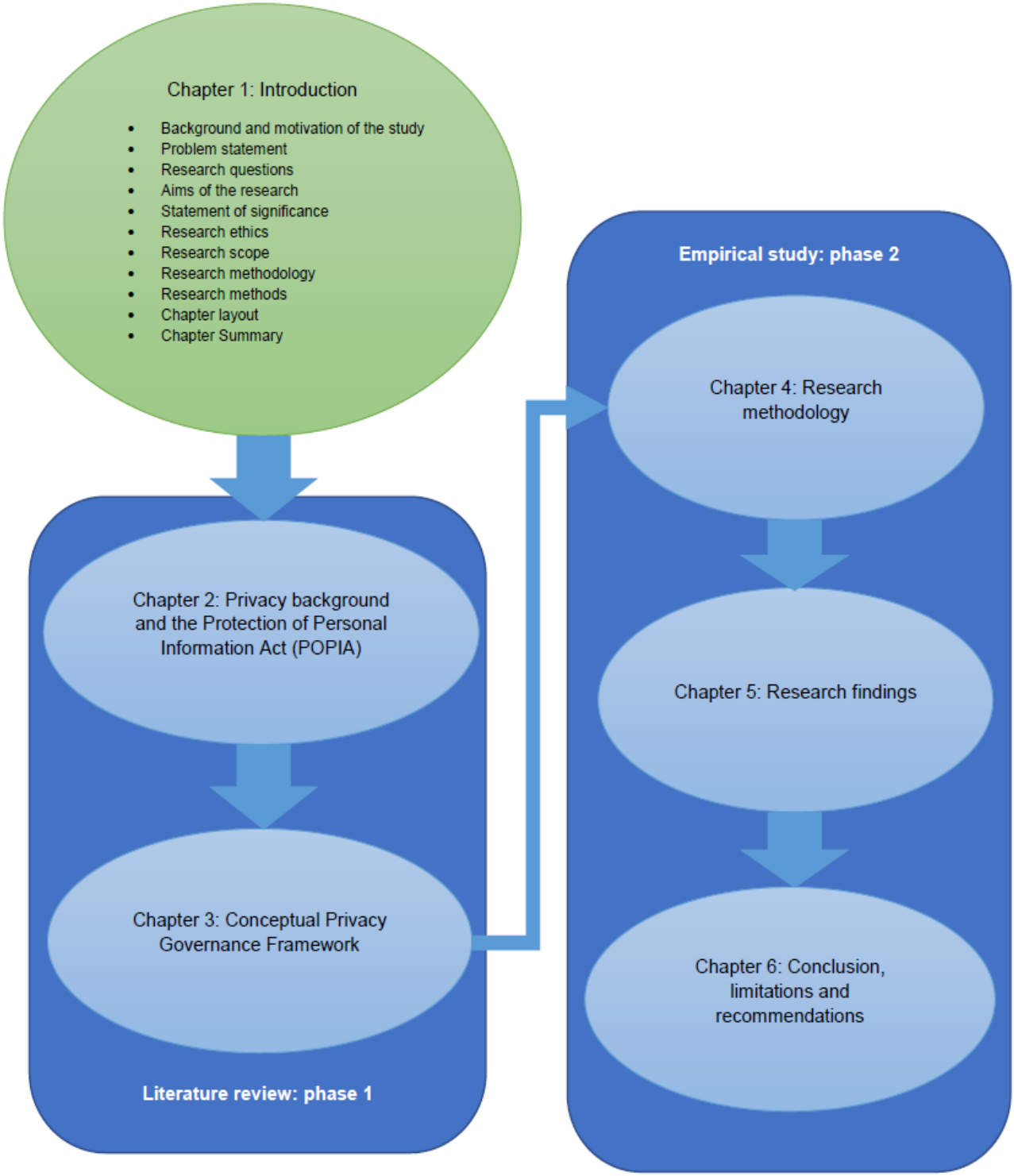
Table of Contents

List of Appendices

List of Figures

List of Tables

CHAPTER 1


Chapter 1: Introduction
Background and motivation of the study
Problem statement
Research questions
Aims of the research
Statement of significance
Research ethics
Research scope
Research methodology
Research methods
Chapter layout
Chapter Summary
Chapter 2: Privacy background and the Protection of Personal Information Act (POPIA)
Chapter 3: Conceptual Privacy Governance Framework
Literature review: phase 1
Empirical study: phase 2
Chapter 4: Research methodology
Chapter 5: Research findings
Chapter 6: Conclusion, limitations and recommendations

Introduction

The main focus of this quantitative study is to develop a conceptual privacy governance framework (CPGF) to govern privacy and a validated questionnaire based on the conceptual framework to measure the perception of how effective privacy is governed within the organisation. This research scope includes Condition 1, Accountability of the Protection of Personal Information (POPIA) Act 4 of 2013, which is a delegated responsibility of the executive management, without abdicating the accountability of the delegated responsibility (King IV Report, 2016). According to the King IV Report, accountability is the "obligation to answer for the execution of responsibilities" (King IV Report, 2016). The organisation must comply with all the conditions and measures that give effect to such conditions while determining the purpose and means of the processing of personal information and during the processing itself (POPIA, 2013).

Chapter 1 discusses the background and motivation of the study, the research questions and aims, as well as the problem statement. It also discusses the paradigm perspective of the research briefly, the research design and research method. The research method describes two phases, namely the literature review phase and the empirical phase. Lastly, the chapter layout is also provided for an overview of the dissertation.

1.1 Background and motivation for the study

The POPIA was signed by the President of South Africa in November 2013 (POPIA, 2013). This Act was promulgated to protect the privacy of individuals when personal information is processed by organisations. Organisations, as responsible parties, must ensure conditions for lawful processing of personal information according to Condition 1 of the POPIA legislation. The responsible party is therefore accountable to protect the personal information and to ensure the lawful processing thereof.

According to Weber (2015), there is a top-down and bottom-up approach, addressing the implementation of regulatory requirements. A top-down approach is when a state executive organ has identified the need for a specific regulation which is then enacted

by legislature. A bottom-up approach is driven by consumers who demand action from legislature with the rise of new technologies, and to ensure protection in this regard (Weber, 2015). The South African government has taken a top-down approach to address the need of privacy and enacted the Protection of Personal Information (POPIA) Act 4 of 2013. While a top-down approach is followed, governments need the joint effort of organisations, individuals and privacy commissioners to take responsibility for the regulation of privacy protection because the pace of technology is increasing (Ernest & Young, 2014).

A strong relationship exists between good governance and compliance with the law (King III Report, 2009). Governance is described as a system or method of management or government (Srivastava, 2009). Dennedy, Fox and Finneran (2014) state that privacy governance is related to an organisation's privacy policy that governs the protection and processing of personal information. Privacy governance is therefore a strategic approach by management to communicate the core values of the processing and protection of personal information to the stakeholder (Dennedy et al., 2014).

A distinction made by the Information Systems Audit and Control Association (ISACA) between privacy governance and privacy management is that privacy governance occurs when the directors of an organisation direct, evaluate and monitor the privacy requirements and vision based on business needs, whereas privacy management occurs when the employees and executive management who are involved with privacy related information focus on the plan as well as the running, building and monitoring of the approach (Vael, 2017).

Tjhin, Vos and Munaganuri (2016) comment that privacy governance is not well-defined in the literature. In their study, they define privacy governance as "the system by which privacy within an entity is directed and controlled" (Tjhin et al., 2016:6). The definition by ISACA addresses the principles of privacy governance and will be used in this study as it incorporates also the terminology of Tjhin et al. (2016).

Privacy governance helps ensuring that employees do their part, and a culture of privacy awareness and accountability are created and maintained (Denham, 2015).

According to Denham (2015), clear accountability policy is a key component of good privacy governance which designates who is responsible for the various functions and aspects of the privacy management programme. The benefit of an effective privacy governance framework will be to identify the personal information and processes the business handles, to determine the risk related to the information and lastly to reduce the risk by implementing controls (Herold, 2005). Privacy governance frameworks assist in creating responsibilities and the necessary roles to maintain and build a privacy-aware and privacy-ready organisation (Dennedy et al., 2014).

Weber (2015) argues that there is no single solution for the protection of personal information and that a multifaceted approach is needed to encompass regulatory measures. A study by Ernest and Young in 2014 focused on privacy in a borderless world and conclude that there is an increase in technological advancements. These technological advancements are *Bring your own device* (BYOD), smartphones and tablets, Web-based applications, cloud computing and social media which all contribute to the borderless world of technology (Ernest & Young, 2014). There is an increase in data collection using technologies across all industries, and regulatory preferences and individuals' privacy-related behaviour is becoming a subject of increased interest by policy-makers, marketers and other societal stakeholders (Miltgen & Smith, 2015).

Organisations sometimes lose sight of their responsibilities and accountability towards regulatory laws because of the focus on improving customer experience (Ernest & Young, 2014). Ernest and Young (2014) argue that privacy should not be an either/or proposition but the ultimate goal should be "and" – security and privacy and technology. The authors recommend, for organisations to achieve this goal, they need to innovate improved policies for the protection of personal information as new technologies emerge.

The IAPP-EY Annual Privacy Governance Report for 2016 shows growing maturity in respect of privacy protection (Hughes & Leizerov, 2016). According to the IAPP-EY survey, privacy awareness is growing, and organisations are establishing privacy departments or appointing privacy officers to implement and govern the organisations'

privacy policies. Privacy policies are part of a privacy governance framework which can aid organisations in the implementation process.

A privacy governance framework clarifies each employee's role in privacy management to ensure that the responsible party is held accountable (Pilgrim, 2014). Privacy frameworks enforce accountability, use on-going compliance monitoring, establish privacy policies, develop automated privacy procedures and manuals, and lastly, they deliver privacy training (Pelkola, 2012). Organisations benefit from effective privacy governance frameworks (Pilgrim, 2014). These benefits are the reinforcement of privacy protection; they ensure compliance with privacy regulations, foster a culture of privacy and enhanced reputation (Office of Privacy Commissioner, 2016). Various frameworks exist – such as the Information and Privacy Commission of New South Wales: Privacy Governance Framework (Pilgrim, 2014); Common Privacy Framework of the Information Privacy Commissioner of Ontario – CCIM Assessment Projects (Community Care Information Management, 2010); Privacy Management Program – The Office of the Privacy Commissioners of Canada, Alberta and British Columbia (Office of Privacy Commissioner, 2016); The Office of the Australian Information Commissioner (OAIC) – Privacy Management Framework (Office of the Australian Information Commissioner, 2015b).

1.2 Problem statement

As mentioned before, the POPIA was promulgated in 2013 with a view to protecting the personal information of data subjects. Responsible parties (i.e. organisations) process, store, update, delete, modify and collect personal information. According to the POPIA, responsible parties must not only have permission for, but can also be held accountable when processing personal information (POPIA, 2013), according to Condition 1 of the POPIA which relates to accountability.

Responsible governance needs must be developed individually in accordance with each cultural and needs-based context (Arnaldi, Quaglio, Ladikas, O'Kane, Karapiperis, Srinivas & Zhao, 2015). In Table 1-1, selected principles from the King IV Report are discussed to highlight the importance of governance and the protection of personal information within an organisation. Principle 3 states that the organisation

must be a *responsible corporate citizen* (King IV Report, 2016), protecting the personal information of the customer. Principle 4 highlights that the governing body should acknowledge that assessment of effective governance gives input to strategic decisions and mitigates risk. Principle 5 indicates that privacy governance assessment is necessary for the stakeholders and governing body to make informed decisions. Principle 9 states that the governing body, through the assessment evaluation, should ensure the effective governance of privacy. Privacy governance frameworks and assessment are necessary for the governing of technology and information, according to principle 12. The governing body should incorporate privacy laws, codes, rules and standards to govern privacy within the organisation, according to principle 13.

Table 1-1: Selected King IV principles

King IV Principles	
Principle	**Description**
3	"Ensure that the organisation is and is seen to be a responsible corporate citizen"
4	"The governing body should appreciate that the organisation's core purpose, its risks and opportunities, strategy, business model, performance and sustainable development are all inseparable elements of the value creation process."
5	"The governing body should ensure that reports issued by the organisation enable stakeholders to make informed assessments of the organisation's performance, and its short, medium and long-term prospects."
9	"The governing body should ensure that the evaluation of its own performance and that of its committees, its chair and its individual members, support continued improvement in its performance and effectiveness."
12	"The governing body should govern technology and information in a way that supports the organisation setting and achieving its strategic objectives."
13	"The governing body should govern compliance with applicable laws and adopted, non-binding rules, codes and standards in a way that it supports the organisation being ethical and a good corporate citizen."

Source: King IV (King IV Report, 2016)

Multiple external norms and demands are continually evolving in the corporate sector to which the corporate privacy activities must respond (Bamberger & Mulligan, 2011). According to Ernest and Young (2013), the POPIA has an impact on functional areas of a business such as its operations, human resources, IT and procurement. Therefore, it behoves companies to

- establish a multi-functional steering committee;
- educate employees regarding privacy awareness;
- conduct a gap assessment; and
- implement a privacy programme with a detailed plan and budget.

Organisations therefore should have a structured approach such as a privacy governance framework to implement privacy across functional areas as well as a method to assess if it has been implemented successfully.

The latest report from a study done by the IAPP-EY Annual Privacy Governance Report 2018 shows that 78% of the respondents acknowledge that privacy is a board-level issue and that the board's concern is long-term privacy compliance (Hughes & Saverice-Rohan, 2018). With the inception of the General Data Protection Regulation (European Union (EU) 2016/679 (GDPR) in March 2018, 56% of the organisations have indicated that they are not compliant with the new legislation. Compared to previous years' survey reports for the preparation for the GDPR, the 2018 report shows a remarkable increase as shown below in Figure 1.1.

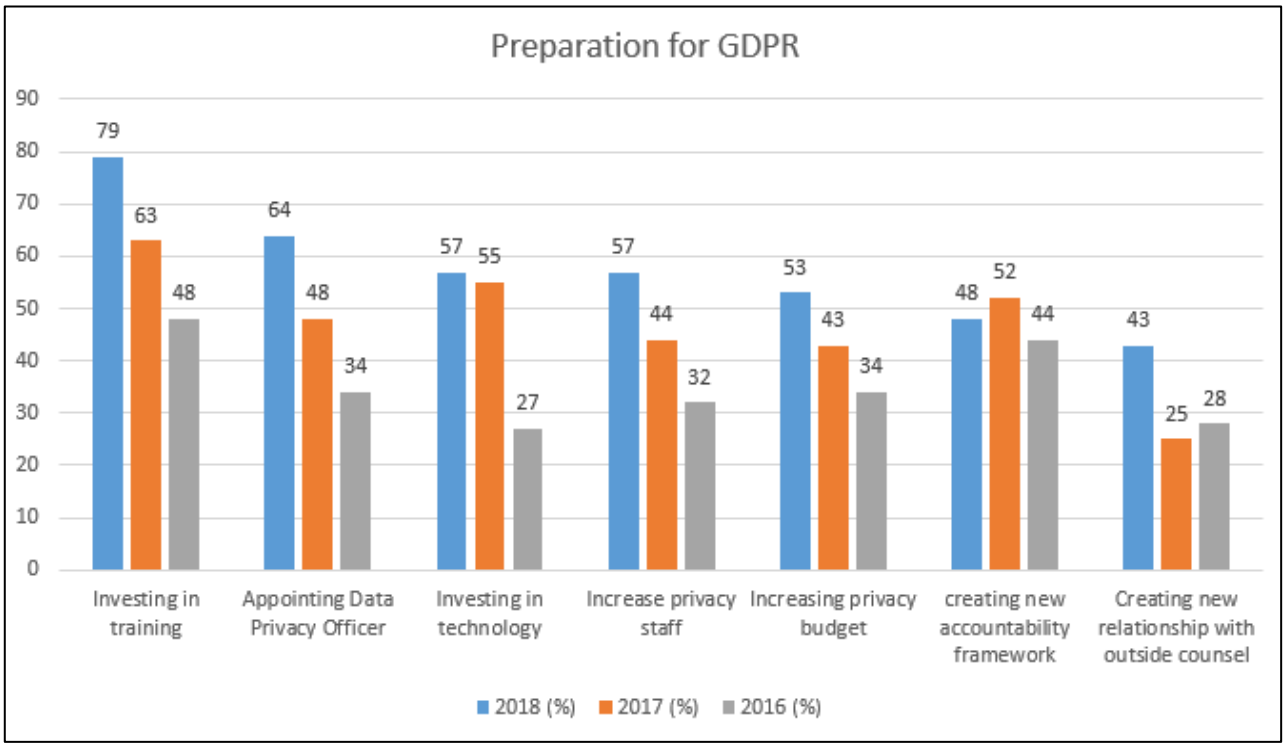


Figure 1-1: Preparation for GDPR (Source: IAPP-EY Annual Privacy Governance Report 2018)

Companies are investing more in privacy training (an increase of 31% since 2016); appointing a data privacy officer (an increase of 30% since 2016); a privacy budget

(an increase of 20% since 2016); and outsourcing privacy counsel (an increase of 15% since 2016) (Hughes & Saverice-Rohan, 2018). PricewaterhouseCoopers (PwC), indicated in a study done in 2017 that the general awareness of employees was still a point of concern, and that there was a strong need for periodic training and awareness campaigns (PricewaterhouseCoopers, 2017).

The IAPP-EY Annual Privacy Governance Report 2018 also features the top privacy responsibilities as shown in Fig 1-2 below. The statistics show that privacy policies, procedures and governance (94%); company privacy-related awareness and training (90%); and privacy-related communication (83%) are among the top three privacy team responsibilities. These statistics indicate that executive management are ensuring compliance with legislation by concentrating more on governance than on other privacy responsibilities such as incident response which have cooled off in 2018. The statistical results of the IAPP-EY Annual Privacy Governance Report 2018 indicate that executive management are assuming accountability for protecting the personal information which they process.

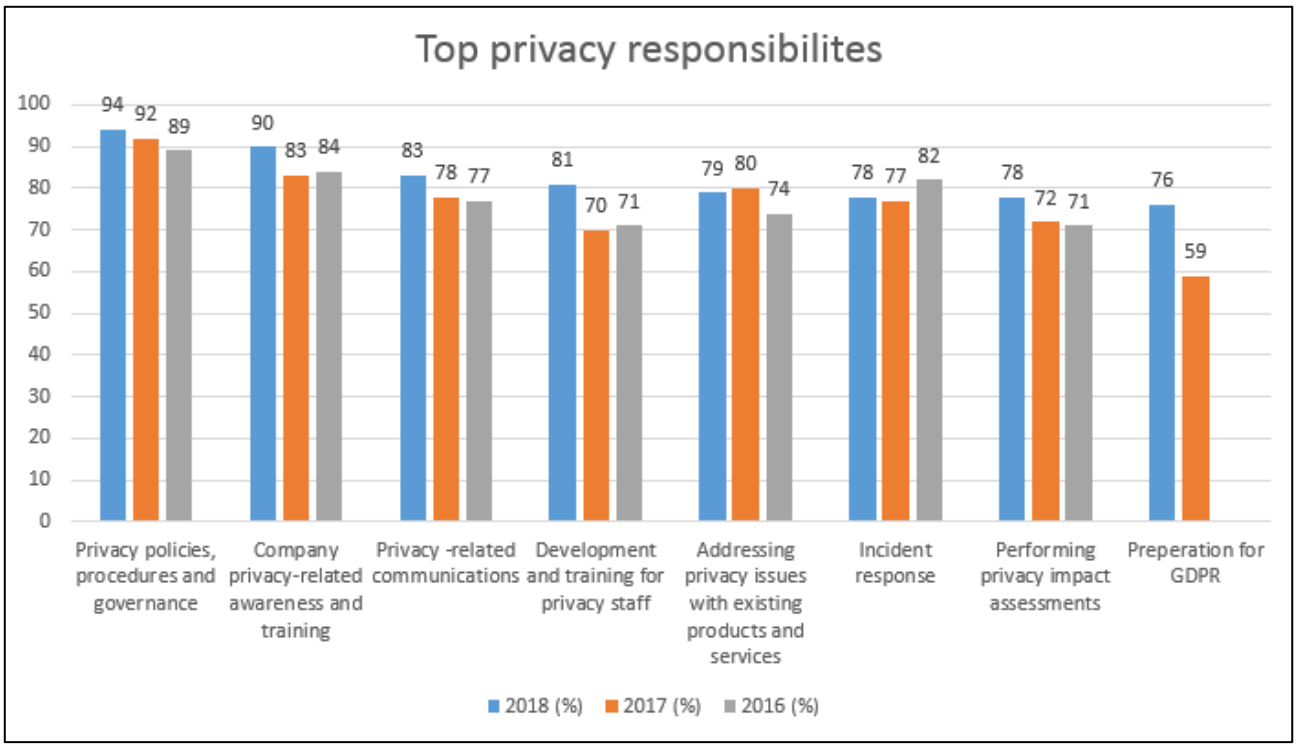


Figure 1-2: Top privacy responsibilities (Source: IAPP-EY Annual Privacy Governance Report 2018)

A study done by Botha, Eloff and Swart (2015) indicates that 56% of small and medium enterprises (SMEs) in South Africa are not sure if they are compliant with the regulations of the POPIA; 12% are in the process of becoming compliant; and 16% are not compliant at all. A survey done by Shred-it (2016) shows that 70% of large organisations in South Africa understand the implications, which the POPIA will have on their businesses, while only 37% of small businesses understand the implications. The Shred-it (2016) survey also indicates that 57% of large organisations have privacy protection protocols in place to which all employees adhere, while 37% of the employees are not aware of the privacy policies that are in place.

From 2012 to 2015, the level of compliance to the POPIA has increased from 44% to 86%, since the Bill has been signed into law and the appointment of the Information Regulator (Dala & Venter, 2016). An experimental study done with insurance companies, which monitored the opt-in, opt-out compliance on the companies' quoting systems, revealed that 42% of the companies did not comply with Section 69 of the POPIA (Swartz & Da Veiga, 2016). The study also revealed that only 25% of the insurance companies had the option to opt-in or opt-out in accordance with Section 69(1) of the POPIA (Swartz & Da Veiga, 2016).

Organisations are not yet compliant in South Africa, and there is a need to give guidance for effective implementation. Globally, a number of countries have compliance processes in place; therefore, South African organisations can follow similar routes and learn from them (Botha et al., 2015).

Raizenberg (2015) indicates that other countries have standards, frameworks and certifications to assist with the development of privacy programmes. In South Africa, there is currently no framework or standard to develop and implement a privacy governance framework, nor guidelines from the Information Regulator. Raizenberg (2015) proposes that the Control Objectives for Information and Related Technologies (COBIT 5), an IT Governance Framework, have proven useful to develop a privacy programme (Raizenberg, 2015). While the privacy programme recommended by Raizenberg (2015) focuses on the POPIA and the eight conditions, it is not aimed at

the governing of privacy, but rather addresses the management of privacy within an organisation.

There is also the ISO 29100 Privacy Framework that consists of the following six components: (i) actors and roles; (ii) interactions; (iii) recognising personal identifiable information; (iv) privacy safeguarding requirements; (v) privacy policies; and (vi) privacy controls (ISO/EIC, 2011). The ISO 29100 Privacy Framework addresses the OECD principles but it is not comprehensive and does not focus on governance.

Given the research results of Botha et al. (2015), a privacy governance questionnaire is needed to assess how effective privacy is governed within the organisation. The impact that the increase of privacy maturity has on South Africa is that organisations must have a privacy department or privacy officers to implement the privacy policies, as well as controls and guidelines to protect and process personal information. Martins and Da Veiga (2015) argue that South Africa may be rated Level 1 (Initial/Ad hoc) according to the Capability Maturity Model (CMM) scale compared to the United Kingdom (UK) with a rating of level 4 (Managed and Measurable) because they are more mature in regulating and implementing the data protection conditions. Hinde (2014) has developed a privacy maturity model called the PoPI Privacy Maturity Model (PoPI-PMM) which measures an organisation's information privacy maturity against the POPIA. Although the PoPI-PMM tool measures the information privacy maturity of the organisation, it does not focus on governance. Therefore, there is a gap for a privacy governance measuring tool to measure the effectiveness of the governance of privacy.

The above-mentioned frameworks do not focus on governance, and there is no assessment instrument available to measure the effectiveness of how privacy is governed within organisations. In South Africa, there is a need for a standard privacy governance framework which will define the privacy roles, impact assessment measures, privacy training and education, incident management, communication structures, privacy review plan and service provider management to govern privacy in organisations.

In summary the main problems identified are:

a. There is no comprehensive privacy governance framework for South African organisations.
b. The available privacy governance frameworks do not focus on the POPIA.
c. There is no assessment instrument that measures how effective privacy is governed within organisations.
d. South African organisations are not compliant yet and therefore there is a need for guidance in the effective implementation of privacy requirements.

1.3 Research questions

Considering the literature background, the following literature and empirical research questions are formulated:

1.3.1 Research questions with regard to the literature review

i. What would a conceptual privacy governance framework comprise?
ii. What would an information privacy governance questionnaire comprise?

1.3.2 Research questions with regard to the empirical study

i. Is the information privacy governance questionnaire (IPGQ) valid and reliable?
ii. What are the employees' views as to how effective privacy in an organisation is governed?
iii. What recommendations and areas for future research, based on the research findings, can be proposed for the improvement of privacy governance in an organisation?

1.4 Aims of the research

From the above problem statement and research questions the following aims have been formulated for the study.

1.4.1 General aim of the study

The general aim of this research is to develop a conceptual privacy governance framework that can be used to develop a valid and reliable information privacy governance questionnaire (IPGQ) to assess the perception of employees on how effective the organisation governs privacy.

1.4.2 Specific aims

1.4.2.1 Research objectives with regard to the literature review

i. To develop a comprehensive privacy governance framework from a theoretical perspective
ii. To conceptualise the dimensions and items of an information privacy governance questionnaire

1.4.2.2 Research objectives with regard to the empirical study

i. To determine the validity and reliability of the information privacy governance questionnaire (IPGQ)
ii. To determine the perceptions of employees in terms of how effective the organisation governs privacy
iii. To suggest recommendations for the improvement of privacy governance in the organisation

1.5 Statement of significance

The significance of the study is to develop a CPGF which can aid organisations to govern privacy in line with the POPIA and their organisational policies. The overall outcome of the study will be a valid and reliable IPGQ to measure the perception of the employees' view on how effective privacy is governed within the organisation.

The contribution for organisations is that the IPGQ can be used to assess how effective privacy is governed and to conduct follow-up assessments to monitor improvements. The IPGQ can also be added to compliance or audit programmes. IPGQ can furthermore be used for comparison studies between industries and organisations to target interventions. The IPGQ can also assist the Information Regulator to give input to prioritise industries with training and awareness. It will also aid the integration of the CPGF into privacy guidelines. Lastly, the IPGQ will serve as the foundation of a valid and reliable questionnaire for future studies.

1.6 Research ethics

This research adheres to the University of South Africa's (UNISA) policy on research ethics to conduct the research responsibly and to protect the rights of the research participants. Ethical clearance has been granted by the university to conduct the research at the financial institution. Various people have participated in this empirical study, namely research participants, expert professionals and colleagues. Permission by the gatekeeper of the financial institution has been granted, and a consent form to participate in the research study has been signed by all participants.

1.7 Research scope

The researcher intends to conduct the research in South Africa who has enacted the POPIA. The targeted organisation for this study is in the financial industry as it processes personal information for various products and services. The study uses Condition 1 of the POPIA which relates to accountability as the basis for this study because the governing body of the organisation is the responsible corporate citizen to protect the personal information it processes.

This study excludes data governance, information security governance and IT governance because the study concentrates on the effective governance of privacy, which includes the direction, monitoring and evaluation of privacy requirements based on the business needs. It also excludes industries such as the health, mining and agricultural industries, as the survey is conducted in a financial institution. Lastly, the study excludes privacy programmes because they are managed by employees and

managers who are involved in the planning, running, building and monitoring of the privacy programmes.

1.8 Research methodology

The research methodology describes the paradigm perspective, research approach, research design and the techniques and procedures in the following sections.

1.8.1 Paradigm perspective

The philosophical paradigm that is considered appropriate for this research study is positivism. Positivism is based on an observable social reality, and focuses on law-like generalisation and causality (Saunders, Lewis & Thornhill, 2016).The researcher's view of the nature of reality is independent and an objective of the social actors (Saunders et al., 2016). The positivist belief is that only observable phenomena allow the researcher to provide credible data (Saunders et al., 2016), and it is also based on precise observations that other researchers can repeat (Neuman, 2014). It incorporates empirical research which derives knowledge from actual experiences based on both observation and measured phenomena (Cahoy, 2016). The ontological assumption of the quantitative paradigm is that there is a singular reality independent from the researcher, and the nature of the reality is objective (Sukamolson, 2007).

In view of the epistemological assumption, the researcher is independent from what will be researched. Questionnaires will be distributed to the respondents without the researcher conducting any interviews or influencing the answering of the questions. The research is value-free, according to the axiology assumption of the paradigm, because the researcher is unbiased, as the researcher's feelings and thoughts will not influence the study. The research process, according to the methodological assumption of the paradigm, describes the process as deductive, accurate and reliable (Sukamolson, 2007). Statistical precision, using statistical software, will ensure the validity and reliability of the data and the findings.

1.8.2 Descriptive research

Descriptive research aims to describe a phenomenon and its characteristics. It concentrates on the “what” research questions (Nassaji, 2015). This type of research method includes comparisons, proper analyses, relationships and the identification of trends (Salaria, 2012). It therefore portrays an accurate profile of situations, persons or events (Saunders et al., 2016).

1.8.3 Research approach

The research approach for this study is the deductive approach. Existing theories derived from the literature or which are developed by the researcher are called the deductive approach (Oates, 2006). Deduction involves rigorous testing to ensure the developed theory is valid and reliable through a series of propositions (Saunders et al., 2016).

1.8.4 Research design

The research design describes the research strategies, research choice and time zone in the following sections.

1.8.4.1 Research strategies

The research strategies guide the researcher to answer the research questions and to reach the objectives of the study (Oates, 2006; Saunders et al., 2016). The choice of research strategy is guided by the research questions, philosophical belief, time, resources and existing knowledge (Saunders et al., 2016). The research strategy that applies to this study is the use of a survey.

Survey research design is the most popular quantitative research design characterised by collecting data, using questionnaires (Muijs, 2004). This type of research entials the gathering of information from the respondents in a systematic pattern to understand and/or predict the behaviour of the population of interest (Sukamolson, 2007). Surveys enable the researcher to collect large amounts of data from the sample population in a cost-effective way (Saunders et al., 2016). The quantitative data collected can be analysed quantitatively by using inferential and descriptive statistics (Saunders et al., 2016). The data collected can therefore be used to explain possible

reasons for relationships between variables and to develop models of these relationships (Saunders et al., 2016).

1.8.4.2 Research choices

There are various research methods which will determine the research design, such as the data collection techniques and the data analysis procedures (Saunders et al., 2016). When choosing the research method, a mono method (single data collection technique with a corresponding analysis procedure) or multiple methods (two or more data collection techniques and analysis procedures) can be used to answer the research questions (Saunders et al., 2016). A quantitative research method is used to collect and analyse the data statistically. This research method makes use of objective research methods which means that the researcher is detached from the research (Muijs, 2004).

The mono method quantitative approach is followed for this research, whereby data is collected during a survey and analysed with statistical methods.

1.8.4.3 Time horizon

Cross-sectional time horizon is used for this study to measure the employee's perception in the organisation regarding information privacy policies and procedures, as business processes change over time.

1.8.4.4 Techniques and procedures

In the following sections, the sampling selection method, data collection technique, expert review, pilot testing, validity and reliability are discussed.

1.8.4.4.a. Sample selection method

A purposive sample (a type of non-probability sample) was used to achieve the objectives of this study (Saunders et al., 2016) because respondents were selected from across the organisational departments to participate in the survey. The purposive sampling technique is normally used with small samples, since the selected sample is particularly informative (Saunders et al., 2016). The participants are selected by virtue of their knowledge or experience, and the researcher decides on the participants who can or are willing to provide the information (Etikan, Musa & Alkassim, 2016). This

sampling technique concentrates on people with particular characteristics (Etikan et al., 2016).

Respondents from different departments (Information Technology (IT), Finance, Marketing, Human Resources (HR), Operations and Privacy) were invited to complete the questionnaire. Approximately five (*n*) respondents are required to complete the questionnaire, where *n* is the total number of questions listed in the questionnaire and five is the value of the point scale (Gerber & Hall, 2017).

1.8.4.4.b. Data collection technique

Varkevisser, Pathmathan and Brownlee (2003) describe a data collection technique as the systematic collection of information about the objects of study and the settings in which they occur. The questionnaire is a method of the data collection technique to collect data. The questionnaire type used for this study is the internet-mediated questionnaire which is a self-administered questionnaire.

1.8.4.4.c. Expert review

To ensure that the questions were relevant and interpreted by all respondents in the same way, a panel of experts reviewed the relevance, clarity and suitability of the questions. The questions were evaluated before the pilot-testing period (Oates, 2006) by experts in the information privacy domain to provide suggestions on the structure of the questionnaire (Saunders et al., 2016).

For this study, the expert panel consisted of four experts from different specialist fields, namely academic and legal as well as a privacy consultant and a compliance officer. Columns were added to the questionnaire for the expert panel, and each statement was evaluated by the expert panel to state if the statement was essential and clear so as to ensure that the respondents would understand and interpret the statements in the same way.

1.8.4.4.d. Pilot testing

Pilot testing is used to refine a questionnaire to improve the comprehension of the questions by the respondents and also to eliminate any problems when recording the data (Saunders et al., 2016). It assists with the assessment of the question reliability and the validity of the data that will be collected (Saunders et al., 2016). Neuman

(2014) suggests that the questionnaire be pilot-tested with a small set of respondents similar to those respondents in the final survey. During the pilot test, the researcher asks the respondents whether the questions are clear, and their interpretations must be scrutinised to determine whether the intended meaning of the question is clear (Neuman, 2014).

In this study, pilot testing was conducted at the financial institution, and administered by the researcher and the academic supervisor. The ten participants of the pilot group completed the questionnaire and an assessment was conducted afterwards to establish if the respondents understood the questions.

1.8.4.4.e. Validity

Validity, as per Saunders et al. (2016:167), confirms whether the research findings "are really about what they appear to be about". When evaluating tests, validity is a crucial consideration, and no findings can be published without validation studies having been conducted (McCowan & McCowan, 1999). The different types of validity are face validity, content validity, criterion-related validity and construct validity (McCowan & McCowan, 1999). Face validity, content validity and construct validity have been applied in this study.

Face validity is defined as a "type of measurement validity in which an indicator makes sense as a measure of a construct in the judgement of others" (Neuman, 2014:216). The construct is really measured by the indicator which is judged by the scientific community (Neuman, 2014). Face validity is tested during pilot testing when the researcher uses an expert panel and a small group of people to pilot-test the questionnaire to determine whether the questionnaire makes sense (Saunders et al., 2016).

Content validity is defined as "a type of measurement validity that requires that a measure represent all aspects of the conceptual definition of a construct" (Neuman, 2014:216). Content validity, therefore, captures the entire meaning (Neuman, 2014).

Neuman (2014) discusses three steps of content validity:

i. The content of a construct definition must first be specified.
ii. All areas of the definition must be sampled.
iii. One or more indicators must be developed to draw from all parts of the definition.

Content validity is tested during the development of the CPGF and the development of the IPGQ. The components of the CPGF and the statements of the questionnaire are substantiated by the content of the literature review.

Construct validity is the “extent to which your measurement questions actually measure the presence of those constructs you intended them to measure” (Saunders et al., 2016:373). An Exploratory Factor Analysis (EFA) is used to determine if the individual questions in the questionnaire load onto the dimensions (Gerber & Hall, 2017). Questions that are part of one construct contribute to that specific construct (Gerber & Hall, 2017). The statistical method used for determining validity in this study is the EFA (Conway & Huffcutt, 2003).

1.8.4.4.f. Reliability

Reliability refers to the internal consistency of item scores on an instrument (Creswell & Creswell, 2017). The consistency of a questionnaire is measured to ensure that consistent findings are produced at different times of a study and under different conditions (Saunders et al., 2016). Since Cronbach’s Alpha Coefficient is the most frequently used method to calculate internal consistency (Saunders et al., 2016), it will be used in the proposed study to measure the reliability of the statistical dimensions or factors. To establish reliability, a score above 0.70 is desirable (Esterhuizen & Martins, 2016). Data collected from a representative sample during a study and trusted statistical software are factors which will aid the reliability of statistical data. Data are stored in an online database and secured with a password, and only the researcher, statistician and supervisors will have access to the online database.

1.9 Research methods

The research has been conducted in two phases, namely Phase 1, which is the literature review phase, and Phase 2 which is the empirical study phase. The research phases are depicted in Figure 1-3 below.

1.9.1 Phase 1: Literature review

The literature review phase consists of the following steps:

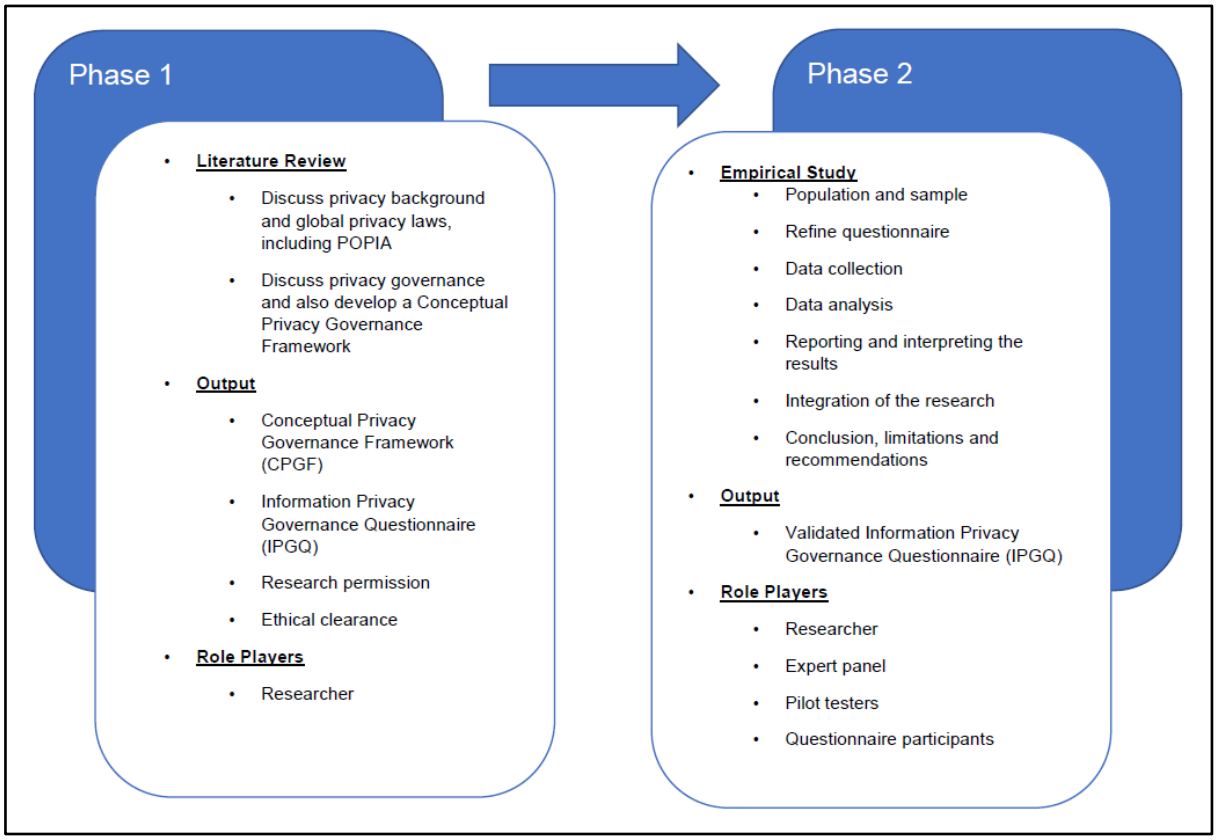


Figure 1-3: Research phases

Step 1 Privacy background is discussed, as well as various global privacy laws. The POPIA and the conditions of the Act are also discussed.

Step 2 Governance is defined. Various governance types are discussed to define privacy governance. A scoping review is performed to identify existing research and components for the CPGF. Various privacy governance frameworks are also discussed to draw a comparison between the frameworks to conceptualise a comprehensive list of the

privacy governance components which will answer research question 1 of the literature review questions.

Step 3 The privacy governance framework and items for the questionnaire to answer research question 2 of the literature review questions are conceptualised.

1.9.2 Phase 2: Empirical study

The empirical study phase consists of the following steps:

- Step 1: Population and sample

  The research study was conducted in a financial institution, as it processed and stored personal information on a daily basis. A purposive sample (a type of non-probability sample) was used to achieve the objectives of this study (Saunders et al., 2016) because the specific organisation and participants from specific organisational departments were selected to participate in the survey.

- Step 2: Development of questionnaire

  The design of the CPGF aided in the understanding of the components that were necessary for constructing the IPGQ. Questions for the questionnaire were generated from concepts in the CPGF and aspects that had influenced users' perceptions. During the development of the questionnaire an expert panel and pilot group assisted with the assessment of the questions. The expert panel reviewed the relevance, clarity and suitability of the questions. The pilot group assisted with the comprehension and clarity of the questions.

- Step 3: Data collection

  The survey was distributed electronically, and the respondents accessed the questionnaire by means of a hyperlink to the survey site. The questionnaire was administered during business hours and no fixed timeframe was set so as to give respondents ample time to complete the questionnaire.

- Step 4: Data analysis

  Data analysis was achieved by means of a statistical analysis which was used to describe, summarise and generalise the results with the greater population as well as to explore the datasets. Validity tests were conducted, using the exploratory factor analysis. Face, content and construct validity were conducted to test the validity of the factors. The Cronbach's alpha coefficient was used to test the reliability of the dimensions or factors, as it was the appropriate method to calculate the internal consistency, thereby answering the first empirical research question.

- Step 5: Reporting and interpreting the results

  The information is presented and summarised in table and graph format by means of descriptive and inferential statistics.

- Step 6: Integration of the research

  The literature review as well as the results of the empirical study are integrated for meaningful interpretation of the results, thereby answering the second empirical research question.

- Step 7: Conclusion, limitations and recommendations

  Conclusion: A summary of the research results as well as the implications are discussed in relation to the objectives of the study that provide an overview of the study, thereby answering the third empirical research question.

  Limitations: The limitations of the research are discussed, and suggestions are made for further research.

  Recommendations: Based on the research results, recommendations for the case organisation are drafted in a report for their perusal.

1.10 Chapter layout

Brief discussions of the chapters (see Figure 1-4) in this dissertation are as follows:

Chapter 1	The research background and motivation are discussed with an outline of the research design and methods.
Chapter 2	Privacy is defined, and global privacy laws are explained. the POPIA is also discussed to provide an overview of the South African privacy laws.
Chapter 3	The term *privacy governance framework* as well as the background of governance are discussed. Various privacy governance frameworks are explained to develop a conceptualised privacy governance framework and questionnaire items.
Chapter 4	The research methodology is discussed for this study. The research approach, research design and the research methods are discussed in detail.
Chapter 5	The research results are discussed. Data are collected and the actual method of data collection is discussed. The collected data are analysed by means of descriptive and inferential statistics. The validity and reliability of the data are also tested and reported.
Chapter 6	This chapter provides the conclusion, limitations and recommendations arising from the research, as possible further studies in relation to the governing of privacy within organisations are proposed.

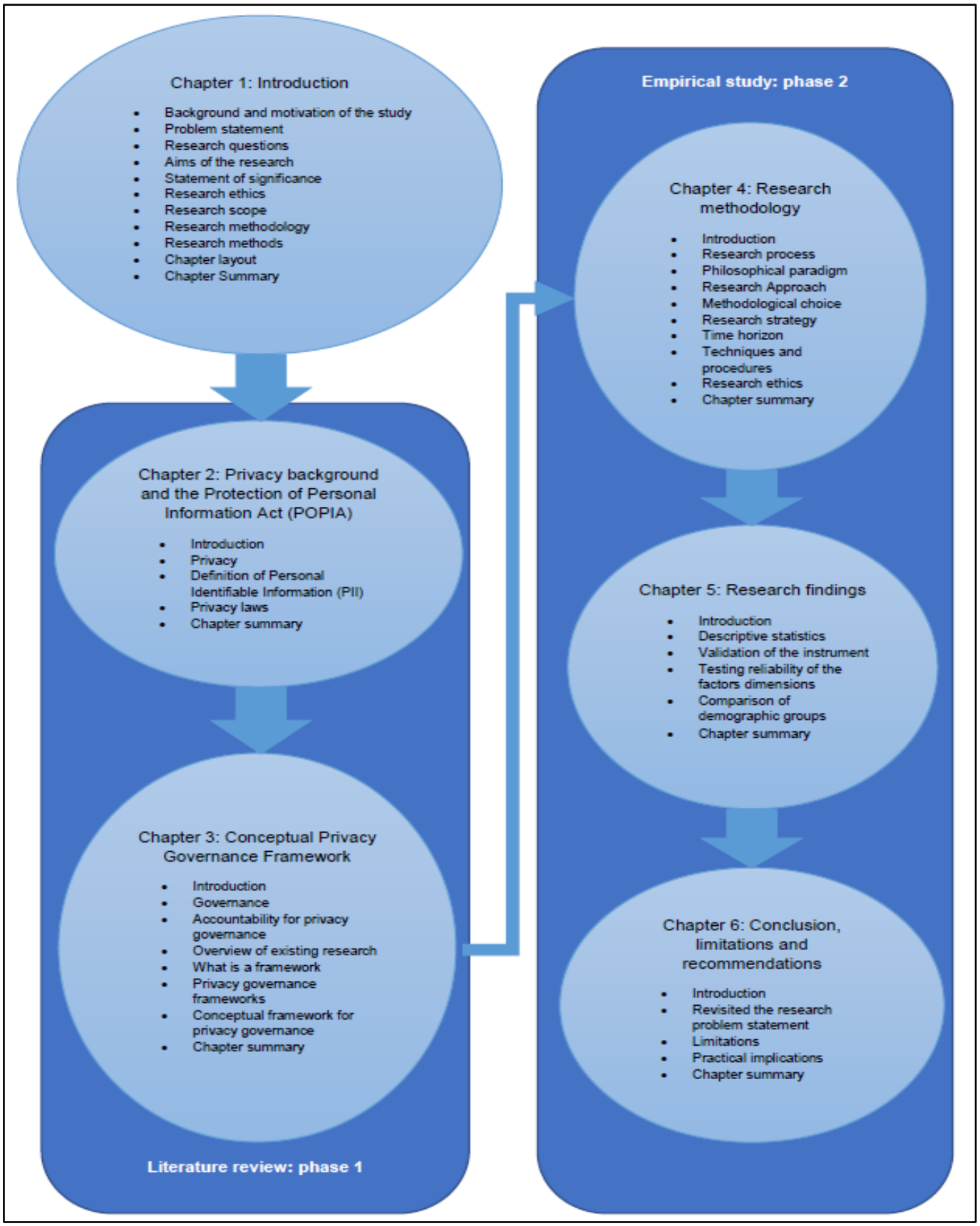


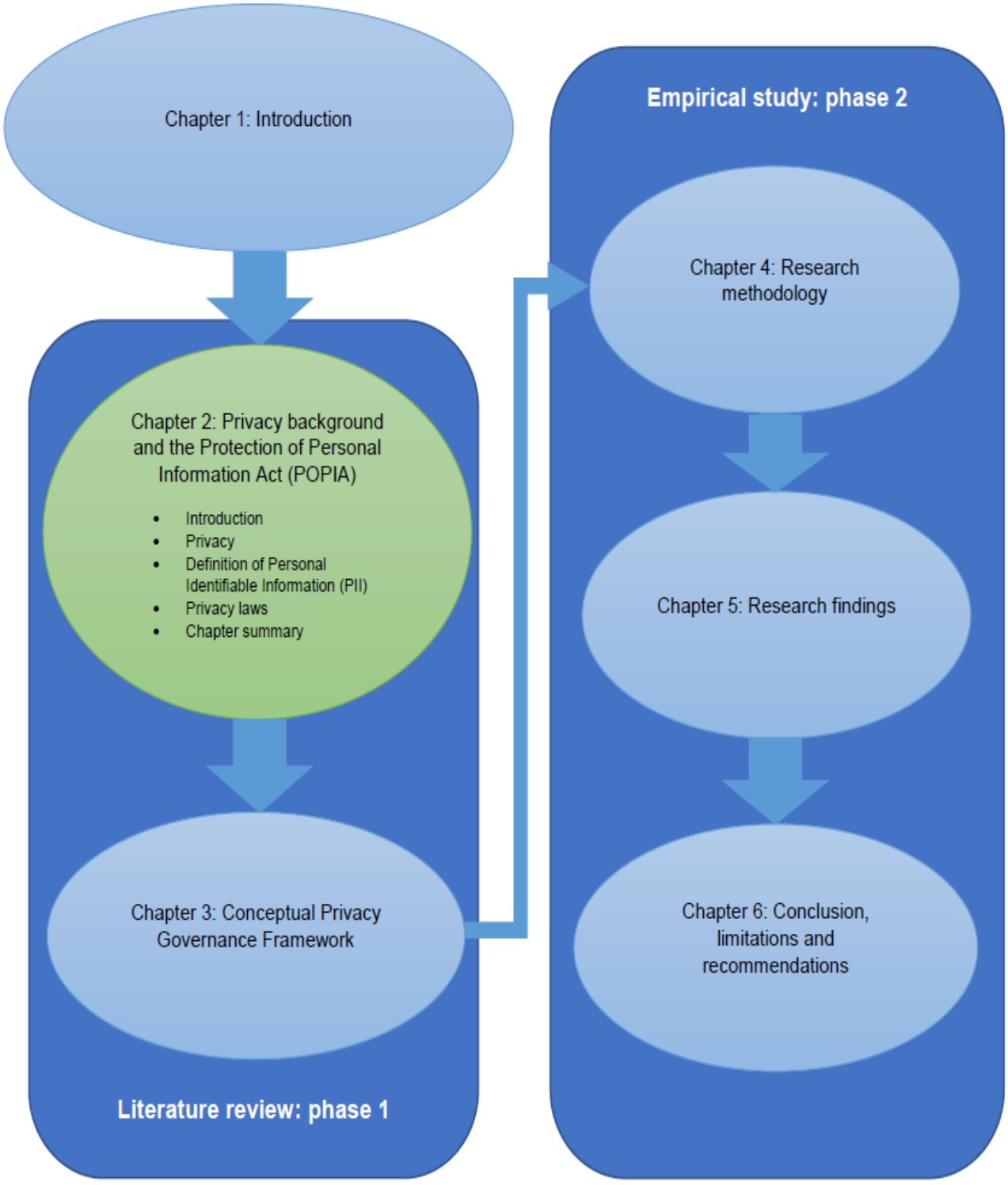
Figure 1-4: Chapter layout

1.11 Chapter summary

The scientific background to the research is discussed in chapter 1. It also introduces the motivation and background for this research. The aims of the study, problem statement, research design and methods as well as the paradigm perspective are discussed to give an overview of the research process.

In chapter 2 that follows, the POPIA and privacy laws as well as the various privacy governance frameworks are discussed.

CHAPTER 2


Chapter 1: Introduction
Chapter 2: Privacy background and the Protection of Personal Information Act (POPIA)
Introduction
Privacy
Definition of Personal Identifiable Information (PII)
Privacy laws
Chapter summary
Chapter 3: Conceptual Privacy Governance Framework
Literature review: phase 1
Empirical study: phase 2
Chapter 4: Research methodology
Chapter 5: Research findings
Chapter 6: Conclusion, limitations and recommendations

Privacy background and the Protection of Personal Information Act (POPIA)

2.1 Introduction

Through history, philosophers, jurists and legal theorists have found it difficult to define the concept of *privacy* (Jordaan & Jordaan, 2004; Solove, 2002). Privacy is an abstract notion to define (Moore, 2008), because it appears to be cultural relative. What may be acceptable in one culture, for example by entering a house or office without knocking is an offense in another culture (Kemp & Moore, 2007).

This chapter will be highlighting the background of privacy where an individual's privacy becomes important and relevant for the broader society. Privacy is also defined and the different types of privacy are discussed. The definition of Personal Identifiable Information (PII) is discussed as a central concept in most global privacy legislation. A high-level overview of the various global privacy laws is provided to indicate how the global society has collaborated to protect the personal information of individuals. The POPIA is also discussed by highlighting the purpose and conditions of the Act.

2.2 Privacy

Privacy is a fundamental human right as per article 12 of the Universal Declaration of Human Rights proclaimed by the United Nations in 1948 (United Nations, 1948). The section below gives an overview of the background of privacy, and discusses the definitions of *privacy* and the types of privacy.

2.2.1 Background to privacy

The early philosophers, Socrates (470-399 BC), Plato (427-347 BC) and Aristotle (384-322 BC) had different views of privacy (Kemp & Moore, 2007). Socrates believed that "The unexamined life is not worth living" and people who had not examined their own lives, he publicly challenged and in some cases, humiliated them (Kemp & Moore, 2007:59). Plato believed that privacy "is inherently disvaluable in relation to the perfect state" (Kemp & Moore, 2007:60).

Privacy legislation has a long history, dating back to the 14th century (Dickie, 2004) when the Justice of the Peace Act was enacted in 1362 in England to punish eavesdroppers (Dickie, 2004).

2.2.2 Definitions of *privacy*

Over the last century, various philosophers like Judge Thomas Cooley (1880) have defined *privacy* as “the right to be let alone”. Privacy, as noted in the United Nations Universal Declaration of Human Rights (1948), is a fundamental human right (Pearson, 2014). Innes (1992:140) defined *privacy* as “the state of possessing control over a realm of intimate decisions, which include decisions about intimate access, intimate information, and intimate action”. The definition of *privacy*, according to Generally Accepted Privacy Principles (GAPP) (AICPA, 2009:4), is “the rights and obligations of individuals and organizations with respect to the collection, use, retention, disclosure, and disposal of personal information”. Since it is a multi-faceted and multidimensional concept, it is hard to contain the concept in a single conceptual setting (Gellert & Gutwirth, 2012).

Analysing the above definitions of *privacy*, the authors refer to privacy as a right that the individual has, and some concentrate on the information control that an individual possesses. The main concepts in most of the definitions (see Figure 2-1) is that an individual possesses the right to decide about the use of his or her personal information and how it is controlled.

The researcher thus defines *privacy* as the right of an individual to possess intimate decisions to control his/her personal information and the processing thereof.

This means that when an organisation collects personal information, it should take cognisance of the regulatory requirements pertaining to privacy as well as the preferences of the customer of how their personal information is processed by the organisation. Ultimately the organisation should have processes in place to govern the processing of the personal information of its customers in order to uphold privacy requirements.

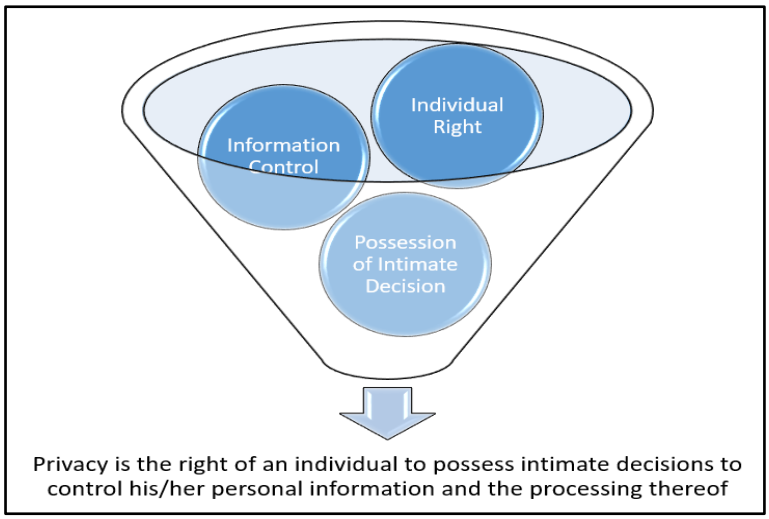


Figure 2-1: Privacy definition (Source – Researcher)

2.2.3 Types of privacy

Privacy is used to signify a number of interests (Kemp & Moore, 2007). These interests include secrecy, personal development, access to places and bodies, personal information control as well as reproductive autonomy.

Finn, Wright and Friedewald (2013) in their study discuss seven types of privacy, namely:

i. "Privacy of the person" – Body characteristics and functions such as biometrics and genetic codes are kept private.
ii. "Privacy of behaviour and action" – Political activities, sexual preferences, religion and habits are sensitive issues.
iii. "Privacy of communications" – This includes mail, telephone or wireless communication interception which must be avoided.
iv. "Privacy of data and image" – Ensure that data or images are not automatically available to organisations or individuals.
v. "Privacy of thoughts and feelings" – Individuals have the right not to share their feelings or thoughts.
vi. "Privacy of association (including group privacy)" – People have the right to associate with whomever they wish without being monitored.
vii. "Privacy of location and space" – Without being monitored, identified or tracked people have the right to move where they want to in public or semi-public spaces.

Solove (2002:1094) argues that privacy can be dealt with under six general headings, namely: “(1) The right to be left alone; (2) Limited access to the self; (3) Secrecy; (4) Control of personal information; (5) Personhood; and (6) Intimacy”. The “privacy of data and image” of Finn et al. (2013) is similar to the “Control of personal information” of Solove (2002), as both argue that an individual must have a certain amount of control over his or her personal information. This control, according to Finn et al. (2013), allows the person to feel empowered and self-confident.

The disclosure, getting hold of personal information or the violation of privacy may constitute an invasion of a person’s private life (Jordaan & Jordaan, 2004). Privacy, therefore, is often categorised in a negative sense and is an intangible commodity (Jordaan & Jordaan, 2004).

Responsible parties (the entities collecting personal information) need to act proactively in protecting the individual’s personal information, and as such his or her privacy, when processing the information, when being confronted by new or emerging technologies and while designing or implementing their policies (Finn et al., 2013).

2.2.4 Taxonomy of privacy

A taxonomy of privacy has been introduced by Solove (2006) to assist the legal system to better understand the concept of privacy relating to personal information when a responsible party processes that information. To effectively evaluate the protection of privacy, one first needs to understand the problems by preventing or redressing the problem (Solove, 2006). Solove (2006) therefore discusses four basic harmful activities (Figure 2.2) in his taxonomy of privacy, namely:

i. Information collection – Surveillance and interrogation
ii. Information processing – The use, storage and manipulation of collected data
iii. Information dissemination – Sharing of information
iv. Invasion – Decisional and intrusion interference

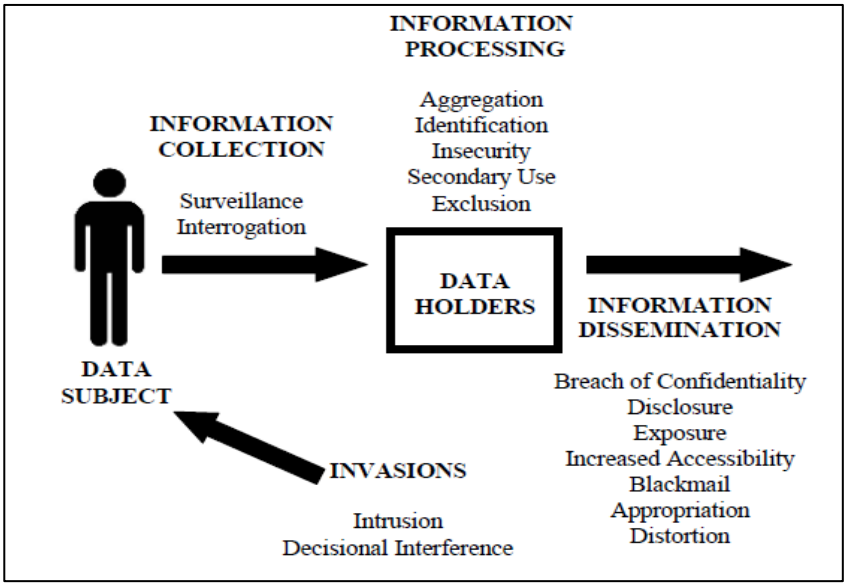


Figure 2-2: Taxonomy of privacy (Solove, 2006:490)

i. The first group of harmful activities for *information collection* is surveillance which entails listening to, watching or keeping information of individuals' activities, whereas interrogation refers to a range of formats of questioning.

ii. The second group of the taxonomy of privacy discusses the activities for the use, storage and manipulation of *information processing*.
   - Aggregation – various pieces of information about an individual which are combined
   - Identification – information which is linked to a specific individual
   - In-security – careless practices of protecting stored information
   - Secondary use – information that is collected and used for another purpose without the individual's consent
   - Exclusion – not informing the data subject about data that third parties have of the individual

iii. The third group of harmful activities in the taxonomy of privacy is *information dissemination*. These information dissemination activities relate to:
   - Breach of confidentiality – dishonouring an oath to safe-keep the personal information

- Disclosure – when the responsible party reveals personal information which impacts the client's character
- Exposure – revealing an individual's feelings or bodily functions. Increased accessibility occurs when disclosing information on the internet because it is already publicised.
- Blackmail – when an individual's personal information is disclosed because of a threat against that person
- Appropriation as a problem – involves the use of an individual's identity for the purpose and interest of another
- Distortion – spreading misleading or false information about an individual

iv. The final group of harmful activities in the taxonomy of privacy is *invasion* which is concerned with intrusion and decisional interference. Intrusion is when an individual's solitude or tranquillity is disturbed by invasive acts, while decisional interference occurs when an individual's decision is determined by government interference.

Personal information could therefore be affected by different harmful activities, and responsible parties (the entities collecting personal information from individuals) need to act proactively in protecting the individuals' personal information when processing it, being confronted by new or emerging technologies and while designing or implementing their policies (Finn et al., 2013).

2.3 Definition of Personal Identifiable Information (PII)

With the rise of computers in the 1960s, Personal Identifiable Information (PII) became evident when private companies and public bureaucracies processed personal data (Schwartz & Solove, 2011). Within information privacy regulations, PII is one of the central concepts (Schwartz & Solove, 2011). Most of the privacy regulations and statutes define *privacy* within the PII scopes and boundaries (Schwartz & Solove, 2011). Personal Identifiable Information is the communal term used in global legislation, while in the POPIA legislation, it is referred to as "personal information" (PI) (Botha et al., 2015).

In general terms, PII is described as (1) “any information that can be used to distinguish or trace an individual’s identity, such as name, social security number, date and place of birth, mother’s maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information” (McCallister, Grance & Scarfone, 2010:39).

The following are examples of PII but are not limited to: (McCallister et al. (2010); POPIA (2013):

- Name, such as maiden name, full name or mother’s maiden name
- Personal identification number, such as passport number, identity number, credit card number or driver’s licence number
- Personal characteristics, including handwriting, biometric data, fingerprints or photographic image
- Address information, such as email address, postal or street address
- Information regarding a person’s medical, financial, employment or criminal history
- A person’s personal preferences, views or opinions
- Individual information that is linked or linkable to any of the above data, such as race, date of birth, activities, place of birth, employment information or medical information

The POPIA legislation defines *personal information* as “information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person”(POPIA, 2013:14). Personal information could relate to:

- Belief, culture, religion, age, marital status, race, gender, sexual orientation, pregnancy, nationality, ethnicity, colour, disability, conscience, physical or mental well-being, birth of the person and language
- Education, financial, criminal, medical or “employment history of the person”
- Any identifying telephone number, location information, number, physical address, email address, online identifier or “any other particular assignment to the person”
- A person’s “biometric information”
- Views, preferences or opinions of a person

- “correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence”
- An individual’s opinion or views about another person
- The name of a person linked to other personal information or if the name is made known which reveals information about the person

The POPIA (2013:15) defines *processing* as “any operation or activity or any set of operations, whether or not by automatic means, concerning personal information”, including:

- The collection, storage, updating, receipt, recoding, collation, organisation or retrieval, consultation, alteration, modification or use
- Information dissemination by means of distribution, transmission or availing it in another form
- Linking, merging, restriction, erasure, destruction as well as degradation of personal information

According to the POPIA (2013:15), *record* means “any recorded information”. The characteristics of a record, according to the POPIA (2013), are as follows:

- It can be any medium or form which can be:
  - Any writing material
  - Recorded, processed or stored by means of computer equipment, tape-recorder, software or hardware or any other device
  - Marking, labelling or other writing that describes or identifies anything to which it forms part or is attached in any way
  - Graphs, drawings, maps, plans or books
  - Tapes, films, photographs, negatives or other devices which embody a visual image which can be reproduced with or without the help of some other device
- Under the control or in possession of a responsible party
- Whether it is produced by a responsible party
- Irrespective of when it is created

Processing of personal information takes place during different stages of the information life cycle (Da Veiga & Martins, 2015). The stages of the information life cycle are described in the following five phases (Da Veiga & Martins, 2015):

i. Collection phase: Customers' information is collected via the internet, application forms and call centres.
ii. Storage phase: Information is stored on media tapes, shared drives, databases or the cloud.
iii. Use phase: Information is processed and used to sell products, deliver services and conduct data analyses.
iv. Retention phase: For legal, regulatory, business, industry and customer requirements, information needs to be retained.
v. Destruction phase: Information which is past its retention period or no more useful is archived and after a while destroyed according to organisational legal requirements and policies.

McCallister et al. (2010) refer to personal information that is traceable to and associated with an individual being in line with that of the POPIA. Non-identifiable information can be turned into identifiable information by technologists (Schwartz & Solove, 2011) which refers to the first part of the McCallister et al. (2010) definition that an individual's identity is traceable. Computers have changed the way in which data are organised, accessed and searched, especially within databases, where computers can be programmed to reorganise or sort data on the foundation of any specific characteristic or index (Schwartz & Solove, 2011). The definition of *personal information*, as defined in the POPIA and explained by McCallister et al. (2010), is used in the context of this research study.

2.4 Privacy laws

In the following sections, global privacy laws, an overview of the General Data Protection Regulation (GDPR) (General Data Protection Regulation [EU], 2016) and the South African privacy law, namely the POPIA, will be discussed.

2.4.1 Global privacy laws

Privacy legislation has a long history as it predates to the 14th century (Dickie, 2004) when the Justice of the Peace Act has been enacted in 1362 in England to punish eavesdroppers (Dickie, 2004). Since 1970, new technologies have been developed at an increasing rate, and because of the combined use of information and technology, the need for the enactment of privacy legislation arose (De Bruyn, 2014).

Globally, privacy laws have increased by nearly 10% since 2015 and reached a total of 120 by January 2017 (Greenleaf, 2017). The National Comprehensive Data Protection/Privacy Laws and Bills Map 2018, compiled by Banisar (2018), is depicted in Figure 2-3 below. It shows the countries in blue that have comprehensive data protection laws. With the update of the map, Brazil, Bahrain, St Kitts and Nevis have been added in 2018 and more than 40 countries have forthcoming bills or privacy initiatives (Banisar, 2018). A similar world map has been created by DLA Piper, a global law firm, that highlights the privacy regulations and enforcements of each country as either heavy, robust, moderate or limited (DLA Piper, 2018). An overview of the various data protection/privacy laws and bills is provided below.

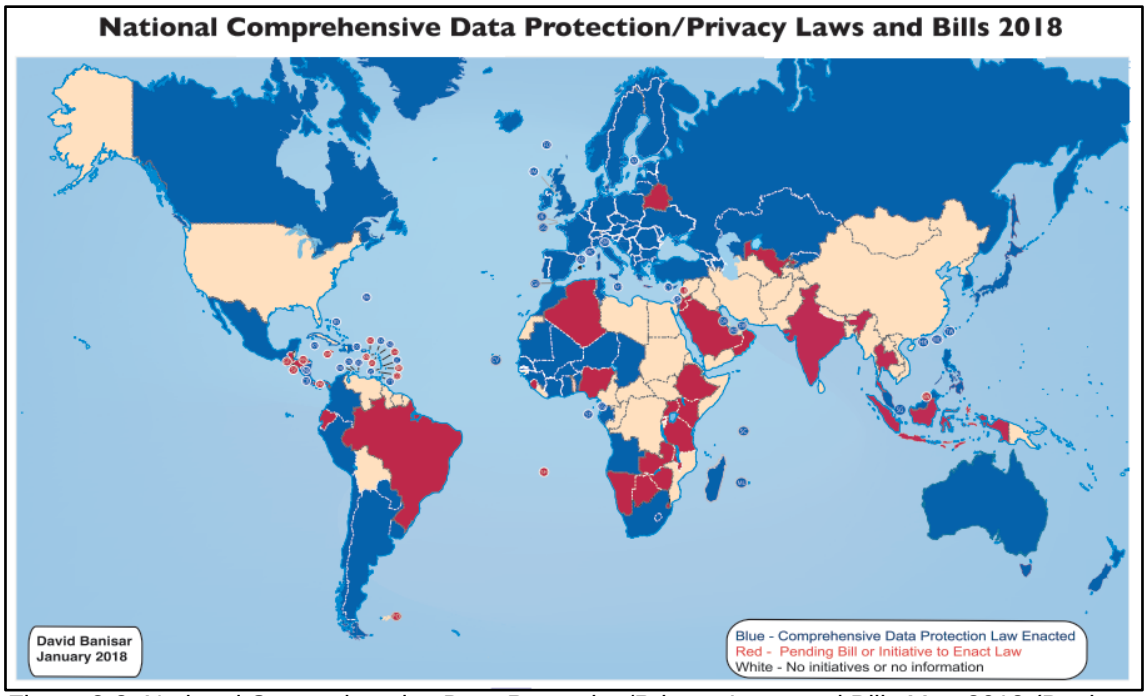


Figure 2-3: National Comprehensive Data Protection/Privacy Laws and Bills Map 2018 (Banisar, 2018)

When the West German State of Hesse enacted the first Data Protection Act in the early 1970s, it was the world's first privacy legislation to be enacted, but it was soon followed by the Data Act of Sweden in 1973 (De Bruyn, 2014). The United Kingdom (UK) implemented its own Data Protection Act (DPA) in 1998, which set out the rules for processing personal information, granted the individual's rights regarding his/her personal information and established a regulatory body to enforce the applicable laws (Bange, Hann, Jefferey & Annereau, 2012). Data protection legislation across the EU was harmonised by the European Commission and by the adoption of the EU's Data Directive 95/48/EC (Bange et al., 2012). The latter directive was updated recently and is now called the General Data Protection Regulation (GDPR) (General Data Protection Regulation [EU], 2016). It addresses the latest technological advances (Allen & Overy, 2018) that are discussed later in the chapter.

The Privacy Act of 1974 of the United States of America (USA) was enforced in September 1975 and characterised as a "code of fair information practices" (Scott, 2015). The Fair Information Practices (FIP) principles are in fact the foundation of the Privacy Act of 1975, and privacy laws in the USA are framed around these principles (Borena, Belanger & Ejigu, 2015). The Act not only has a "No disclosure without consent" rule, but also acknowledges the right of a data subject to apply for the amendment of records if they are incorrect, irrelevant or incomplete (Scott, 2015). The USA does not have an all-inclusive privacy protection policy but follows a sectorial approach to privacy (Park, 2007). A sectorial approach to privacy refers to privacy laws that are aimed at a particular privacy sector (Park, 2007). The Federal Trade Commission (FTC) has been enforcing information privacy policies since 1990 and is to date the most influential regulating body as a sectorial privacy law in the USA (Solove & Hartzog, 2014). The Health Insurance Portability and Accountability Act (HIPAA), as a sectorial privacy law, has been enacted on 21 August 1996. Its main objective is to control the use and disclosure of protected health information by responsible parties (Clearwater & Hughes, 2013).

Australia has enacted its Privacy Act in 1988 (Australian Government, 1988). This Act includes thirteen Australian Privacy Principles (APPs) that apply to government agencies as well as to some private sector organisations (Australian Government, 1988). The principles mainly address how personal information must be used, handled

and managed. Personal information must also be disclosed for direct marketing purposes, and cross-border disclosure of personal information is also addressed in the principles (Australian Government, 1988).

In Africa, certain countries have constitutional articles hinting at the general protection of personal information (Borena et al., 2015). For instance, Tunisia, following the lead of South Africa, has enacted laws for the protection of data that are derived from the EU Data Protection Directive (Borena et al., 2015). Other African countries such as Angola, Algeria, Cape Verde, Ethiopia, Ghana, Gambia, Kenya, Zimbabwe, Uganda, Egypt, Eritrea, Central African Republic, Republic of Congo, Djibouti and Guinea-Bissau have provisions regarding privacy that were decreed at constitutional level (Borena et al., 2015).

2.4.2 General Data Protection Regulation (GDPR) overview

An overview of the GDPR will be provided for this section because, according to De Bruyn (2014), data protection requirements of the POPIA are similar to the Data Protection Directive which has been enacted in 1995. It has been updated since and is now known as the GDPR (Baloyi & Kotze, 2017). An overview of the GDPR is discussed because the financial institution has a GDPR clause in its privacy policy to which employees must adhere when processing EU data subjects' personal information and also when the EU data subjects request the data to be transferred to another party.

The GDPR is applicable to the European countries as per Section 3 of Article 2, Chapter 1 of the GDPR regulation which states in its material scope that it applies to the processing of personal data by the EU offices, bodies, institutions and agencies (General Data Protection Regulation [EU], 2016). New obligations for data subjects are imposed in the GDPR such as data subject consent, data security standards, the right to be forgotten and the EU-wide breach notification rules (Hughes & Leizerov, 2016). The Data Privacy Officer (DPO) is also mandatory and must be a subject matter expert of data protection law (Wolters, Koorn & Koetsier, 2016). Under the GDPR, organisations must now demonstrate that organisational and technical measures, which ensure the protection of personal data, are continuously reviewed and updated

(Wolters et al., 2016). The GDPR legislation was enacted on 24 May 2016 (Michalsons, 2017) and came into force on 25 May 2018 (Hughes & Saverice-Rohan, 2018).

The objective of the GDPR is to provide guidelines to protect the processing of personal data of a natural person as well as the free movement of personal data. The regulation also protects an individual's right to the protection of personal data and the freedom of a natural person. The material scope of the regulation describes the processing means of the personal data, albeit automated or by means of a filing system. The territorial scope of the regulation discusses the processing of personal data in the EU, whether the personal data has been processed in the EU or not in the context of the activities of the organisation (General Data Protection Regulation [EU], 2016).

The GDPR discusses seven principles for the processing of personal data (General Data Protection Regulation [EU], 2016):

i. Lawfulness, fairness and transparency – The personal data of the data subject must be processed legally, fairly and transparently.
ii. Purpose limitations - Personal data must be collected for a legitimate, explicit and specified purpose.
iii. Data minimisation – For the purpose of which personal data have been processed, it must be relevant, adequate and limited.
iv. Accuracy – The personal data must be kept up to date and accurate, and inaccurate data must be rectified or erased without delay.
v. Storage limitations – Personal data that identify an individual must be stored in a form for no longer than is necessary for the purpose it has been processed.
vi. Integrity and confidentiality – Personal data must be protected against unlawful or unauthorised processing, destruction or damage, accidental loss, using secure and appropriate organisational or technical measures.
vii. Accountability – The controller is accountable for the personal data and has to comply with the regulations of the GDPR.

These principles closely resemble the conditions in the POPIA in South Africa. The definitions are also similar to those of the GDPR, such as the data protection officer and the information officer respectively (Giles, 2016).

2.4.3 Protection of Personal Information Act 4 of 2013, South Africa

In November 2013, the Protection of Personal Information Act 4, 2013 (POPIA) was signed by the president of South Africa. A proclamation was later made in the Government Gazette of 11 April 2014 to immediately implement Sections 1, 112, 113 and Part A of Chapter 5 of the POPIA to appoint an Information Regulator (Information Regulator South Africa, 2017).

2.4.3.1 Purpose of the POPIA

The POPIA focuses on four purposes to ensure the lawful processing of personal information, namely (POPIA, 2013):

i. To safeguard personal information administered by the responsible party which gives effect to the constitutional right to privacy. It ensures that there are justifiable limitations which aim to ensure (1) a balance between the right to privacy and other rights such as the right of access to information, called the Promotion of Access to Information Act (PAIA), Act No. 2 of 2000; and (2) that important interests, such as the free flow of information across international borders and within South Africa, are protected.
ii. Conditions are set to regulate the way in which personal information is processed in concordance with international standards.
iii. The legislation provides the individual with remedial action and the right to protect his or her personal information if it is processed unlawfully.
iv. It establishes the Information Regulator to fulfil, promote and enforce the rights protected by this Act.

2.4.3.2 Scope of the POPIA

The POPIA is divided into chapters which discuss each aspect of the Act in detail. The first two chapters discuss the definitions of the terminology used in the Act as well as the purpose of the Act, and provides an introductory overview of the Act. The third chapter discuss the conditions for the lawful processing of information, the processing

of special information and also the processing of personal information of children. The exemptions from conditions for processing personal information are discussed in chapter 4. Supervision is discussed in chapter 5 which outlines the establishment, duties, powers and functions of the Information Regulator.

The Act also discusses prior authorisation for the processing of personal information from the Information Regulator other than for the purpose it has been collected. The codes of conduct are also discussed. These codes incorporate all the conditions for the processing of personal information and how it must be applied or complied with. The rights of the data subject are discussed regarding direct marketing by means of unsolicited electronic communication, directories and automated decision-making. Furthermore, the trans-border information flow requirements are outlined, describing the rights of the responsible party when transferring personal information outside of South Africa. The last three chapters of the legislation discuss the enforcements of procedure for handling complaints, offences, penalties, administrative fines and general provisions.

2.4.3.3 Conditions of POPIA legislation

The principles of the POPIA are based on the principles contained in privacy legislation of the EU, thus the GDPR, and in the document called “The OECD Privacy Framework” of the Organisation for Economic Cooperation and Development (OECD) (OECD, 2013) which has been recommended to Parliament by the South African Law Reform Commission (SALRC) (Heyink, 2011). Furthermore, the conditions of the POPIA legislation are derived from the OECD privacy principles which are largely accepted by most countries who have privacy laws enforced (OECD, 2013).

The POPIA states eight conditions for the “lawful processing of personal information (Heyink, 2011; POPIA, 2013), namely:

Condition 1: The responsible party must be accountable to ensure conditions for the lawful processing of personal information.

Condition 2: Limitations for the processing of personal information lawfully and in a reasonable manner.

Condition 3: The personal information must be collected for a specific purpose and the data subject must be aware of the purpose.

Condition 4: Further processing limitations for the collection of personal information must be in accordance with the purpose.

Condition 5: The quality of personal information collected by the responsible party must be accurate, updated, not misleading and complete.

Condition 6: The responsible party must be transparent by maintaining all documentation for the processing operations for which it is responsible.

Condition 7: When processing personal information, the responsible party must have security measures in place for the integrity and confidentiality of personal information.

Condition 8: Data subjects have the right to participate, when providing proof of identity, to request information held by the responsible party or proof that the responsible party has processed their personal information.

The scope of this study relates specifically to Condition 1. Condition 1 prescribes that the responsible party, in other words, the organisation, must be held accountable when processing personal information lawfully (POPIA, 2013). According to the OECD principle and the POPIA condition of accountability, the responsible party must comply with all the conditions and the measures that give effect to such conditions (OECD, 2013; POPIA, 2013). Accountability is the obligation of the organisation to act responsibly and disclose the results in a transparent manner. Accountability requirements also relate to aspects such as that an organisation must appoint a privacy officer to supervise the privacy protection programme during its development, implementation and maintenance phases. There must also be policies and processes in place for the processing and protection of personal information, and for dealing with training and privacy awareness (Office of Privacy Commissioner, 2016). Privacy of

personal information is governed by the organisation's privacy policies which include the guidelines, rules and standards (Dennedy et al., 2014).

2.4.3.4 Status of the POPIA

The Information Regulator has since been established and the office bearers of the Regulator have been appointed by the president of South Africa, effective from 1 December 2016 (Information Regulator South Africa, 2016). The commencement date of the POPIA, once the president has proclaimed the date, gives organisations a one-year grace period to comply with the POPIA (Michalsons, 2017). South African businesses, however, still have time to put policies, procedures and privacy frameworks in place, as the POPIA has not been fully implemented yet (De Bruyn, 2014).

2.5 Chapter summary

This chapter highlighted the background of privacy, where an individual's privacy became important and relevant for the broader society. The concept of privacy indicated that it started around 400 BC when a natural person's privacy became prevalent. The first privacy legislation dates back to the 14th century. Various privacy definitions have been highlighted which denote that a natural person has the right to be left alone, has control over his or her information and possesses control over his or her intimate decisions relating to the processing of their personal information. Different types of privacy were discussed that described the characteristics of privacy. Definitions of PII were discussed as well as how the POPIA defined *personal information*.

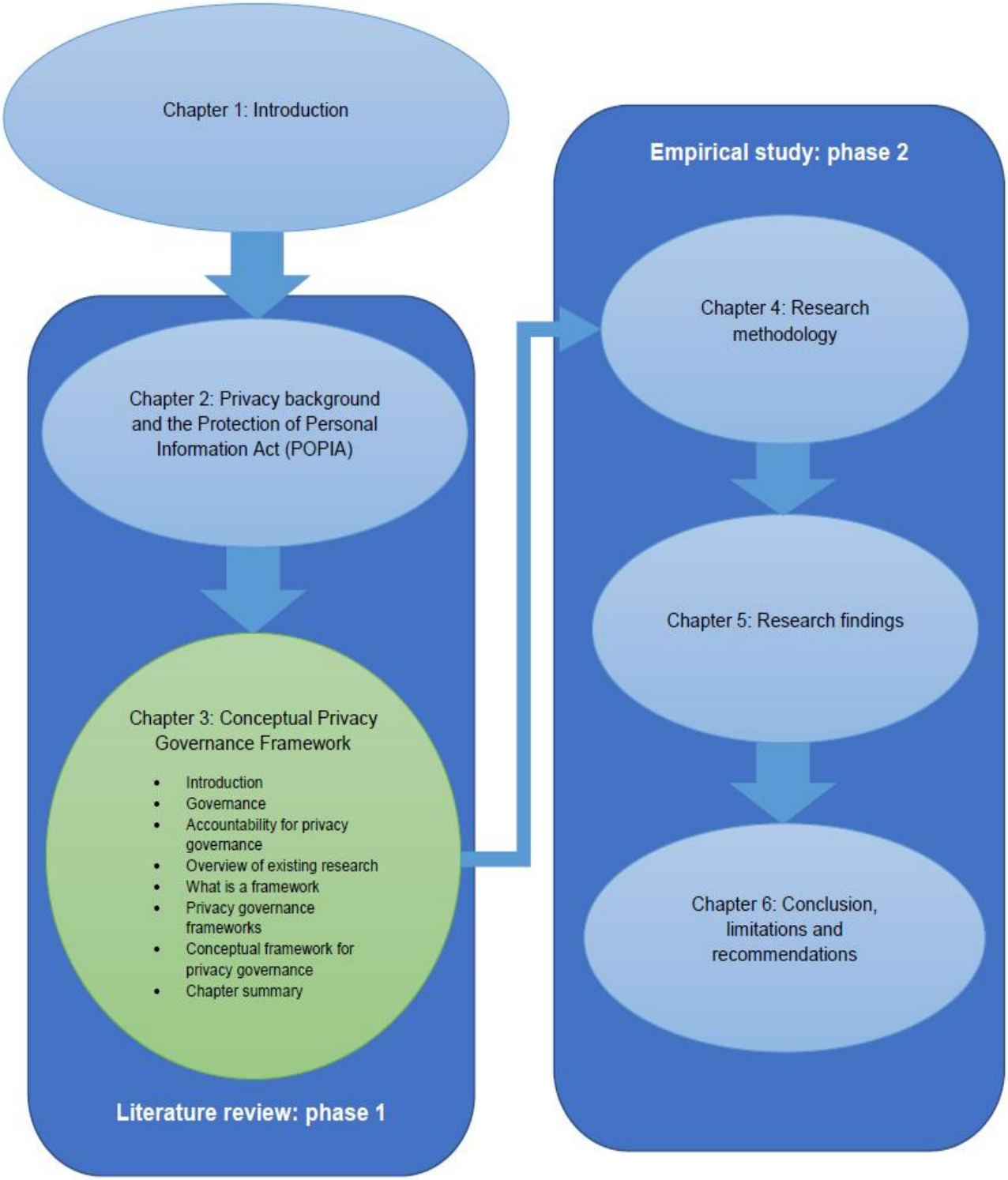
The definition applicable to this study is that of the POPIA and the definition by McCallister et al. (2010) that states that any information can be traced to an individual identity and any information can be associated with an individual.

By 2017, 120 countries have already adopted privacy laws, according to Greenleaf (2017) and recently, the EU has updated the EU Data Directive to a data protection regulation, called the General Data Protection Regulation (GDPR). This regulation has been enacted to comply with the changing privacy activities globally.

An overview of the POPIA was also discussed, namely the purpose, scope, conditions and status of the legislation.

In the next chapter, privacy governance will be discussed which highlights the accountability of the responsible party to ensure conditions and all the measures to lawfully process personal information in accordance with Condition 1, accountability in the POPIA and other related privacy legislation such as the GDPR. Literature regarding privacy governance and the related frameworks will also be reviewed to develop the CPGF, and from the CPGF components, the IPGQ statements will be formulated.

CHAPTER 3


Chapter 1: Introduction
Chapter 2: Privacy background and the Protection of Personal Information Act (POPIA)
Chapter 3: Conceptual Privacy Governance Framework
Introduction
Governance
Accountability for privacy governance
Overview of existing research
What is a framework
Privacy governance frameworks
Conceptual framework for privacy governance
Chapter summary
Literature review: phase 1
Empirical study: phase 2
Chapter 4: Research methodology
Chapter 5: Research findings
Chapter 6: Conclusion, limitations and recommendations

Conceptual Privacy Governance Framework

3.1 Introduction

The commitment of leadership towards a culture of privacy is a key component for good privacy governance (Office of the Australian Information Commissioner, 2015b). This chapter provides an overview of governance as well as the definitions of corporate governance, IT governance, data governance and privacy governance. The meaning of the word *framework* is described as well as the term *privacy governance framework*. A scoping review is conducted to identify important privacy governance components for the conceptual privacy governance framework (CPGF). Privacy governance frameworks are furthermore discussed and the similarities identified to derive the components that can be used to develop the CPGF. The chapter concludes with the proposed CPGF and a discussion of the components, thereby addressing the literature research question one, namely "What would a conceptual privacy governance framework comprise?"

3.2 Governance

In this section, definitions of the concept of *governance* are discussed to provide an overview as well as the integral components of governance, such as corporate governance, information technology governance and data governance.

3.2.1 What is governance?

The Oxford online dictionary defines governance as "the action or manner of governing a state, organisation, etc." (Oxford Online Dictionary, 2017:1). Governance denotes all processes of governing, whether undertaken by a market, network or government, whether over an informal or formal organisation, family or tribe, and whether through power, laws, language or norms (Bevir, 2012). Governance, therefore, focuses on social activities and practices (Bevir, 2012).

The role of governance is to give overall directions to the organisation, satisfying the legitimate expectations for regulations and accountability by the interests beyond the

corporate boundaries, and it is therefore not concerned with the running of the business within the organisation (Rhodes, 1996).

Good governance, according to the King III Report (2009), states that it is about effective leadership. The King IV Report is effective since 1 April 2017 (Clamp, 2017) and concentrates on ethical and effective leadership (King IV Report, 2016). Such leadership is characterised by the ethical values of transparency, fairness, responsibility and accountability, and based on moral duties (King III Report, 2009). Company strategies and operations are directed by responsible leaders with a view to achieve social and environmental as well as sustainable economic performance (King III Report, 2009). Governance, therefore, contributes to the effectiveness and efficiency of the organisation (Klievink, Bharosa & Tan, 2016).

In the paragraphs to follow, corporate governance, information technology (IT) governance and data governance will be discussed briefly to give a high-level overview of the different types of governance frameworks within an organisation.

3.2.2 Corporate governance

Corporate governance is defined as “the system of checks and balances, both internal and external to companies, which ensures that companies discharge their accountability to all their stakeholders and act in a socially responsible way in all areas of their business activity” (Solomon, 2007:15). The central role of corporate governance is to provide accountability within the organisation (Pearson, 2014). Pearson (2014) suggests that accountability is achieved by the identification of risks by the organisation, having appropriate policies in place to mitigate risk and mechanisms to enforce internally for monitoring that these mechanisms are effective within the organisation, and lastly, by validating the internal and external actions. According to Klievink et al. (2016), governance establishes an agreement on the procedures and standards which will guide the activities of the organisation. Frameworks and guidelines assist in creating necessary responsibilities and roles to ensure that the organisation builds and maintains a privacy-aware and ready organisation (Dennedy et al., 2014).

The King III and King IV Reports define *corporate governance* as "the exercise of ethical and effective leadership by the governing body towards the achievement of the following governance outcomes: ethical culture; good performance; effective control; legitimacy" (King III Report, 2009; King IV Report, 2016). A comparison of the King III and King IV governance components are highlighted in Table 3-1 below. The 17 principles are also portrayed in the table which are linked to the governance components of the King IV Report.

Table 3-1: King III Report: Governance components

King III Governance Components	King IV Governance Components	King IV Principles
1. Ethical leadership and corporate citizenship	Leadership	1. "The governing body should lead ethically and effectively."
	Organisational ethics	2. "Govern the ethics of the organisation in a way that supports the establishment of an ethical culture."
	Responsible corporate citizenship	3. "Ensure that the organisation is and is seen to be a responsible corporate citizen."
Refer to 9. Integrated Reporting and Disclosure	Strategy and performance	4. "The governing body should appreciate that the organisation's core purpose, its risks and opportunities, strategy, business model, performance and sustainable development are all inseparable components of the value creation process."
	Reporting	5. "The governing body should ensure that reports issued by the organisation enable stakeholders to make informed assessments of the organisation's performance, and its short, medium and long-term prospects."
2. Board's and directors' roles and 3. Audit committees	Primary roles and responsibilities of the governing body	6. "The governing body should serve as the focal point and custodian of the corporate governance in the organisation."
	Composition of the governing body	7. "The governing body should comprise the appropriate balance of knowledge, skills, experience, diversity and independence for it to discharge its governance role and responsibilities objectively and effectively."
	Committees of the governing body	8. "The governing body should ensure that its arrangements for delegation within its own structures promote independent judgement, and assist with balance of power and the effective discharge of its duties."
	Evaluation of the performance of the governing body	9. "The governing body should ensure that the evaluation of its own performance and that of its committees, its chair and its individual members,

		support continued improvement in its performance and effectiveness."
	Appointment and delegation to management	10. "The governing body should ensure that the appointment of, and delegation to, management contribute to role clarity and effective exercise of authority and responsibilities."
4. The governance of risk	Risk governance	11. "The governing body should govern risk in a way that supports the organisation in setting and achieving its strategic objectives."
5. The governance of information technology	Technology and information governance	12. "The governing body should govern technology and information in a way that supports the organisation setting and achieving its strategic objectives."
6. Compliance with laws, rules, codes and standards	Compliance	13. "The governing body should govern compliance with applicable laws and adopted, non-binding rules, codes and standards in a way that it supports the organisation being ethical and a good corporate citizen."
	Remuneration governance	14. "The governing body should ensure that the organisation remunerates fairly, responsibly and transparently so as to promote the achievement of strategic objectives and positive outcomes in short, medium and long term."
7. Internal audit	Assurance	15. "The governing body should ensure that assurance services and functions enable an effective control environment, and that these support the integrity of information for internal decision making and of the organisation's external reports."
8. Governing stakeholder relationships	Stakeholder relationships	16. "In the execution of its governance roles and responsibilities, the governing body should adopt a stakeholder-inclusive approach that balances the needs, interests and expectations of material stakeholders in the best interests of the organisation over time."
9. Integrated reporting and disclosure	*Refer to Reporting*	*Refer to Principle 5*
	Responsibilities of institutional investors	17. "The governing body of an institutional investor organisation should ensure that responsible investment is practiced by the organisation to promote the good governance and the creation of value by the companies in which it invests."

Source: King III and King IV Reports (King III Report, 2009; King IV Report, 2016)

Within the King IV Report, most of the governance components of the King III Report have been separated into individual governance components, such as the "Ethical leadership and corporate citizenship" (King III Report, 2009) which has been

separated as “Leadership”, “Organisational ethics” and “Responsible corporate citizenship” (King IV Report, 2016). “Strategy and performance” as well as “Remuneration governance” has been added in the King IV report. “Information technology governance”, as in the King III Report (2009), has been separated as two distinct components in the King IV Report, because technology is the source of business opportunity and disruption while information needs to be secured against any risk (King IV Report, 2016).

For this study, the King IV Report for corporate governance is of relevance, as it addresses governance outcomes and the accountability of the governing body to promote ethical culture and legitimacy. The King IV Report’s key aspects are outcome-based, “apply and explain” while 16 of the 17 principles are applicable to any organisation. The King IV Report also addresses the relevance of protecting the privacy of personal information as noted under the practices of 12th principle of the report (King IV Report, 2016) which is in line with the POPIA requirements.

3.2.3 IT governance

“IT governance is the organisational capacity exercised by the Board, executive management and IT management to control the formulation and implementation of IT strategy and in this way ensure the fusion of business and IT” (Steenkamp, 2011:2). According to Steenkamp (2011), governance of IT has a need to comply with external regulations, which is the primary driving force behind it (Steenkamp, 2011). Overall performance and cost-efficiency increase by practising good governance (Steenkamp, 2011). According to the King III Report, to achieve sustainable social and environmental performance, effective governance of information must be in place (King III Report, 2009).

According to the National Computing Centre (2005:6), “IT governance is an ongoing activity that requires commitment from high-level management to respond and improve the policies and guidelines in a fast changing IT environment.” IT governance spans the organisation, practices, culture and policy that manage IT, and controls five key areas (National Computing Centre, 2005):

i. Alignment – Strategic direction is provided to align IT with the business with regard to projects and services.
ii. Value delivery – Maximum business value is derived from IT to oversee the delivery of value to the business.
iii. Risk management – This ensures that risks have been managed adequately to ascertain that processes are in place.
iv. Resource management – IT resources are sourced and used by providing high-level direction.
v. Performance measurement – Strategic compliance is verified by achieving strategic IT objectives.

The benefits of effective IT governance are transparency and accountability in order to improve IT costs, IT portfolio and IT processes as well as return on investment or stakeholder value (National Computing Centre, 2005). The conditions of the POPIA require a responsible party to be accountable and transparent when processing personal information (POPIA, 2013).

IT governance, therefore, supports the increasing regulatory and legal requirements of corporate governance, and is integrated within a wider enterprise governance approach (National Computing Centre, 2005). A survey done by IAPP-EY (2016) indicates that privacy teams are most likely to work with information technology teams for 74% of the time, which is third in rank after information security (87%) and legal (80%) teams.

The definition of Steenkamp (2011) is the focal point of this study, as it addresses the importance of the accountability of the governing body as well as the responsibility of IT management to align the IT strategy with the business objectives and external legislation.

3.2.4 Data governance

Data governance is defined “as a strategic, top-down program for data management in which an organisation leadership communicates the core value of data quality and integrity to stakeholders” (Dennedy et al., 2014:53). Thomas (2006:3) defines data

governance as “the exercise of decision-making and authority for data-related matters”. It is, therefore, a system of accountabilities and decision rights to process information implemented according to mutual agreed models which outline the actions to be taken, with what information and when (Thomas, 2006). Data governance requires data stewardships and stewards who are responsible for the use and value of data, and also the development and implementation of procedures and standards (Dennedy et al., 2014).

The Data Governance Institute (DGI) refers to ten universal data governance components for the data governance framework as depicted in Figure 3-1 below (Thomas, 2006).

Figure 3-1: DGI Data governance framework (Source: Thomas [2006])

In Figure 3-1, the first six components refer to the rules and rules of engagement. Components 7, 8 and 9 refer to the people and organisational bodies, while component 10 refers to the processes of data governance.

The second component of the data governance framework refers to governance metrics and measures which relate the measures that must be in place to fulfil the conditions of the POPIA for the lawful processing of personal information. Component 5 of Figure 3-1 refers to accountability which also refers to Condition 1 of the POPIA. Component 6 of the framework includes controls which are preventive, detective and corrective in nature and relate to Condition 7 of the POPIA to secure and protect personal information. The POPIA describes the responsibilities of the Information Officer which relate to Component 8 (data governance office) of the data governance framework. This officer will resolve privacy issues, monitor privacy compliance and provide privacy training. Component 10 is also very important to monitor and evaluate the governance processes, policies, controls and compliance with privacy legislation.

3.2.5 Privacy governance

A distinction made by the Information Systems Audit and Control Association (ISACA) between privacy governance and privacy management is that privacy governance is implemented when the governing body of an organisation directs, evaluates and monitors the privacy requirements and vision according to the business strategy, whereas privacy management occurs when the executive management and employees who are involved with personal information focus on the process of the privacy programme such as to plan, run, build and monitor the programme (Vael, 2017). Tjhin et al. (2016) define privacy governance as “the system by which privacy within an entity is directed and controlled”. The latter definition will be incorporated into the distinction made by the ISACA who states that directors of the organisation are accountable to evaluate, monitor and direct the privacy requirements and vision based on the business needs.

Privacy governance helps ensuring that employees do their part, and that a culture of privacy awareness and accountability is created and maintained (Denham, 2015). According to Denham (2015), a clear accountability policy is a key component for good

privacy governance which designates who is responsible for the various functions and aspects of the privacy management programme.

3.2.6 Summary of governance definitions

In Figure 3-2 below, the four governance definitions discussed above are depicted. Corporate governance, IT governance, privacy governance and data governance inherit similarities from the governance definition and also from one another.

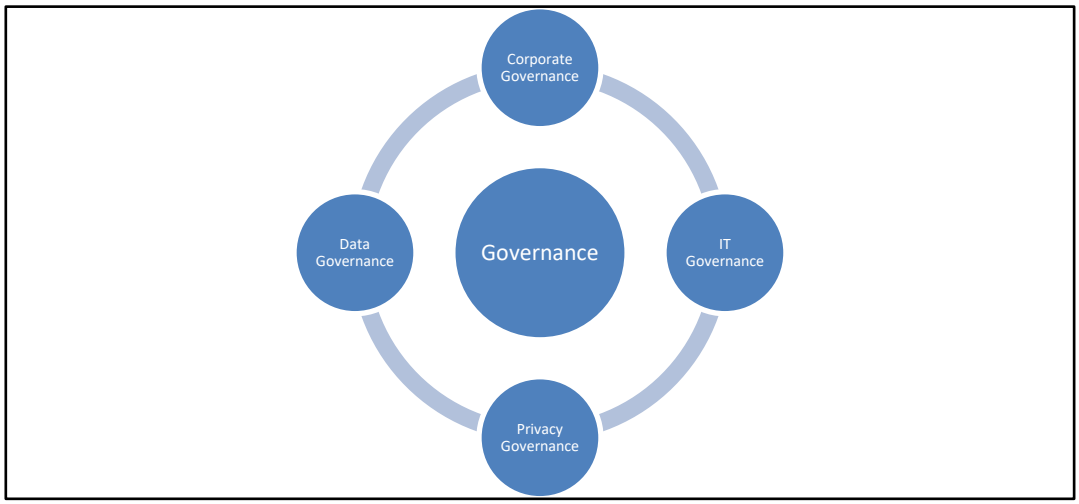


Figure 3-2: Governance definitions (Source: Researcher)

As discussed earlier on in this chapter, governance provides direction and ensures that the policies, procedures and standards comply with legislation. It also ensures accountability from leadership (Rhodes, 1996). Each concept entails separate governance aspects but similar principles apply, such as accountability, performance measurement, evaluation, risk and incident management. The main focus for this study is on privacy governance.

Though there are distinct differences between corporate, IT, data and privacy governance, there are common components that highlight their similarities. All governance frameworks require organisational commitment, which, in turn, requires that leadership of the organisation be committed and accountable. There must be governance offices and a governance officer to ensure that the policies are implemented effectively and reports generated for the different stakeholders. Policies must be developed by the governing body, and governance controls are implemented to ensure that the policies are executed successfully. All frameworks require ongoing

reviews of the policies, processes and controls in place, and also that assessments are conducted to ensure compliance with regulatory laws.

3.3 Accountability for privacy governance

In the realm of privacy and data protection, accountability is fast becoming a fashionable notion among scholars, privacy activists and regulators (Bennett, 2012; Raab, 2012). The accountability movement was started in 1981 by the Organisation for Economic Co-operation and Development (OECD) as an instrument to promote data protection (Raab, 2012). Felici and Pearson (2015:9) state that “accountability consists of defining governance to comply in a responsible manner with internal and external criteria, ensuring implementation of appropriate actions, explaining and justifying those actions and remedying any failure to act properly”. According to the fourteenth guideline of the OECD, “(a) data controller should be accountable for complying with measures which give effect to the principle of accountability” (Raab, 2012:16) while Bennett (2012:33) opines that “accountability implies a process of transparent interaction in which that body seeks answers and possible rectification”.

The growing trend to govern modern science and technology responsibly started a few decades ago in diverse fields like technology and ethics assessment (Arnaldi et al., 2015). According to Arnaldi et al. (2015), responsible governance needs to be developed according to each cultural and needs-based context. Accountability is more than responsibility and responsiveness because it must be directed towards an external agent who holds stakeholders accountable for their actions (Bennett, 2012). In the reporting structure of organisations, privacy officers are required to report to government agencies and stakeholders while the compliance level regarding policies, laws, social norms and regulation is determined by these actors (Klievink et al., 2016).

Accountability increases trust, improves organisational operations (Pearson, 2012) and creates a culture of responsibility among staff members (Butin & Le Metayer, 2015). Raab (2012) argues that accountability is a proactive measure – it does not wait for a system failure but requires the organisation to be prepared for whenever the authorities require proof that data are secure and well-protected in accordance with the essential components. In addressing accountability, the first condition of the

POPIA is also affected; however, organisations require guidance, such as a privacy governance framework, to implement accountability.

The benefit of an effective privacy governance framework will be to identify the personal information and processes the business handles, to determine the risk related to the information and lastly, to reduce the risk by implementing controls (Herold, 2005). Privacy governance frameworks assist in creating responsibilities and the necessary roles to maintain and build a privacy-aware and privacy-ready organisation (Dennedy et al., 2014).

The next section focuses on a literature review that has been conducted in order to define the components for the CPGF.

3.4 Overview of existing research

A scoping review was conducted to identify existing academic literature for *privacy governance* frameworks. A scoping review provides a preliminary assessment of the scope and size of the potential available research literature (Grant, Booth, & Centre, 2009). The reason for this review is to identify the extent and nature of the research evidence (Grant et al., 2009). It provides a comprehensive summary of synthesize evidence with the objective to inform practices, policy and programs and also to provide direction for future research (Colquhoun et al., 2014). As such the scoping review was used to identify existing privacy governance frameworks, components that can be used to develop a privacy governance framework and related privacy governance assessments such as a questionnaire.

An electronic search was done for “Privacy Governance” OR “Privacy Governance Framework” OR “Privacy Program” OR “Privacy Management Program” OR “Privacy AND Measure AND Questionnaire” OR “Privacy AND Maturity AND Questionnaire” OR “Privacy AND Assessment AND Questionnaire” OR “Privacy AND Maturity AND Assessment” OR “POPI AND Measure AND Questionnaire” OR “POPI AND Maturity AND Questionnaire” OR “POPI AND Assessment AND Questionnaire” OR “POPI AND Maturity AND Assessment” OR “Privacy governance AND Measure AND Questionnaire” OR “Privacy governance AND Maturity AND Questionnaire” OR

“Privacy governance AND Assessment AND Questionnaire” OR “Privacy AND Maturity AND Assessment”. The search was conducted from 2000 to 2018 in the IEEE Explore, SpringerLink and ProQuest academic databases. The three databases provided scholarly journals for the scientific and social sciences community. The search was limited to only scholarly articles and journals. The results of the scoping review are listed in Table 3-2.

Table 3-2: Scoping review search

Search keywords	“Privacy Governance” OR “Privacy Governance Framework” OR “Privacy Program” OR “Privacy Management Program” OR “Privacy AND Measure AND Questionnaire” OR “Privacy AND Maturity AND Questionnaire” OR “Privacy AND Assessment AND Questionnaire” OR “Privacy AND Maturity AND Assessment” OR “POPI AND Measure AND Questionnaire” OR “POPI AND Maturity AND Questionnaire” OR “POPI AND Assessment AND Questionnaire” OR “POPI AND Maturity AND Assessment” OR “Privacy governance AND Measure AND Questionnaire” OR “Privacy governance AND Maturity AND Questionnaire” OR “Privacy governance AND Assessment AND Questionnaire” OR “Privacy AND Maturity AND Assessment”			
	Electronic Databases			**Total**
	IEEE Xplore https://ieeexplore.ieee.org/Xplore/home.jsp	**SpringerLink** https://link.springer.com/	**ProQuest** www.proquest.com/	**3** **electronic databases**
Total articles searched	68	44	127	**239**
Total relevant articles for analysis	1	0	3	**4**

From the searches, 239 articles were identified which addressed the searched keywords and details regarding a privacy governance framework or the measuring of privacy governance. After reviewing the 239 articles, duplicates and articles mentioning the searched keywords but which do not contribute to privacy governance, privacy governance frameworks or the measuring of privacy governance were removed. The articles removed therefore did not discuss a privacy governance framework as such, nor the components of a privacy governance framework nor measurement. Some articles did not contribute any insight to a specific privacy

governance issue (methodology, further research or topic). Four articles were identified for further analysis because they had addressed privacy governance or essential components for a privacy governance framework. The authors of the four articles suggested components that were essential for an effective privacy governance framework but did not propose an actual privacy governance framework. No articles were identified that addressed privacy governance measurement.

The following sections give an overview of the components identified in the four articles that are important for effective privacy governance and which can be integrated into a privacy governance framework.

3.4.1 Delgado

Delgado (2011) suggests that, apart from a data governance framework and security and compliance frameworks, organisations must have a dedicated privacy programme. Delgado (2011:376) identifies the following components for effective privacy governance:

- “A formal privacy governance structure
- Written policies and practices
- Funding for privacy efforts
- Designated point of contact for privacy issues
- Formal procedure for receiving and resolving inquiries and complaints
- Data inventories and classification
- Risk assessment
- Privacy impact assessments
- Education and awareness
- Privacy audits
- Regulatory awareness”

3.4.2 Herold

Herold (2005) argues that, for an organisation to build an effective privacy governance programme, the organisational leaders must know their business. For a business to be successful, privacy and security precautions as well as trust are essential and inevitable components. According to Herold (2011), a privacy governance framework

must be built around policies, processes, people, training and awareness. Herold (2005) suggests the following components for an effective privacy governance programme:

- Establish a privacy leader.
- Implement clear privacy policies.
- Educate all employees and business partners.
- Establish controls (authorisation, technical, access and process) that support privacy policies.
- Monitor compliance and regulations.
- The PII the organisation handles must be documented and defined.
- Establish privacy incident response procedures.
- Report a privacy environment to the governing body and stakeholders.

3.4.3 Seerden, Salmela and Rutkowski

Seerden, Salmela and Rutkowski (2018) analysed five papers regarding privacy governance. The study summarised the privacy governance requirements for organisations and how management could be proactive in responding to privacy issues. According to Seerden et al. (2018), there was a need for a standardised audit process or privacy governance framework which would assist organisations to comply with the GDPR. Seerden et al. (2018) analysed the literature and identified the following components for a privacy governance framework:

- Ascertain the relevance of the data the organisation collects.
- Create a privacy policy.
- Designate an individual responsible for information protection.
- Educate personnel on information protection.
- Ensure data access controls.
- Ensure data security.
- Ensure the correctness of data.
- Ensure the deletion of data.
- Identify databases and the processing of data.
- Inform individuals on the use of their personal information.
- Take precautions to limit damage in case of privacy issues.
- Track physical data location.

3.4.4 Weber

According to Weber (2014), organisations must develop a strategy to comply with privacy regulatory requirements. Organisations must implement appropriate privacy governance frameworks tailored according to their business needs which will be suitable and efficient for their business requirements. Weber (2014:291) suggests the following components for a privacy governance:

- "Maintain governance structure.
- Maintain personal data inventory.
- Maintain data privacy policy.
- Embed data privacy into operations.
- Maintain training and awareness programmes.
- Maintain information security risk.
- Manage third-party risk.
- Maintain notices.
- Maintain procedures for inquiries and complaints.
- Monitor new operational practices.
- Maintain a data privacy breach management programme.
- Monitor data handling practices.
- Track external criteria."

The components of privacy governance frameworks of the four articles show that there are similarities among the proposed components. The seven components that are similar in all the articles are:

i. The appointment of an individual responsible for the protection of personal information
ii. Implementation of privacy policies
iii. Privacy training and awareness programmes for all employees of the organisation
iv. Privacy controls which must be in place
v. Data inventories
vi. Risk management
vii. Privacy incident management

None of the four articles propose a structured framework for privacy governance, but only discuss the individual components. These components will be considered when developing the CPGF.

3.5 What is a framework?

It is important to understand the underlining concepts of a framework. The general term for a framework is defined as a supporting structure which is a basis for something being constructed (The Free Dictionary Online, 2017). The theoretical meaning of a framework is defined differently for each subject matter. In the Cambridge Online Dictionary, framework is defined as “a system of rules, ideas, or beliefs that is used to plan or decide something”. This definition for framework is mainly used within the legal system to resolve disputes. According to the Oxford Online Dictionary (2017:1), framework is defined as “a basic structure underlying a system, concept, or text. An example is the theoretical framework of political sociology”. The Free Dictionary Online (2017:1) defines framework as “a set of assumptions, concepts, values and practices that constitutes a way of viewing reality”. For this study, the latter definition of framework will be used as the basis for the privacy governance framework that will be conceptualised. A framework, therefore, assists in our thinking and communication about uncertain and complicated concepts which provide clarity and purpose (Thomas, 2006).

3.6 Privacy governance frameworks

In this section, various privacy governance frameworks are discussed to identify the main components of each of the frameworks. A comparison table is created to highlight the similarities and differences of each privacy governance framework.

A privacy governance framework clarifies each employee’s role in privacy management to ensure that the responsible party is held accountable (Pilgrim, 2014). Privacy frameworks enforce accountability, use ongoing compliance monitoring, establish privacy policies, develop automated privacy procedures and manuals, and lastly, they deliver privacy training (Pelkola, 2012).

Pearson (2012) states that best practice in a privacy programme requires support from senior management, the establishment of clear processes and delegation of duties to individuals, the utilisation of existing standards and the establishment of monitoring and audit practices. It is difficult to assess whether all the privacy guidelines or criteria of a privacy programme have been implemented successfully when there is no privacy framework in place (Kroener & Wright, 2014). Organisations benefit from effective privacy governance frameworks (Pilgrim, 2014). These benefits are reinforcement of privacy protection, ensuring compliance with privacy regulations, fostering a culture of privacy and an enhanced reputation (Office of Privacy Commissioner, 2016).

Various privacy governance frameworks exist, namely the:

- Information and Privacy Commission of New South Wales: Privacy Governance Framework (Pilgrim, 2014);
- Common Privacy Framework of the Information Privacy Commissioner of Ontario – CCIM Assessment Projects (Community Care Information Management, 2010);
- Privacy Management Program – The Office of the Privacy Commissioner of Canada (Office of Privacy Commissioner, 2016); and
- The OAIC – Privacy Management Framework (Office of the Australian Information Commissioner, 2015b).

These privacy governance frameworks were identified on the internet on the relevant government's privacy commissioner's websites and were found to be the most prominent. The Privacy Management Program of the Office of the Privacy Commissioner for Personal Data, Hong Kong (PCPD) was excluded because it was modelled on the framework of the OIPC (Office of Privacy Commissioner, 2016) which included the same key components. The EU who enacted the GDPR in May 2018, had not developed a privacy governance framework as of yet.

The next section gives an overview of each of the four privacy governance frameworks.

3.6.1 Information and Privacy Commission of New South Wales: Privacy Governance Framework

The Information and Privacy Commission (IPC) of New South Wales (NSW) in Australia has developed a privacy governance framework to assist local councils, universities or NSW agencies to customise their own robust privacy governance frameworks for their organisations (Pilgrim, 2014). The IPC's privacy governance framework is based on the Privacy and Personal Information Protection Act of 1998 (PPIP Act) which defines the individual's right, the roles of the Privacy Commissioner and also the responsibilities of agencies (Pilgrim, 2014).

The IPC framework consists of five components that influence one another in a chronological sequence. The components of the framework are as follows:

- Element 1: Setting leadership and governance
- Element 2: Planning and strategy
- Element 3: Programme and service delivery
- Element 4: Complaint incident management
- Element 5: Evaluating and reporting

The IPC privacy governance framework identifies the following key functions and roles (Pilgrim, 2014):

- Audit and Risk Committee and security experts – Ensure risk frameworks consider privacy risk, and monitor and identify privacy breaches
- Privacy Control Officer – Responsible for developing procedures, privacy management plans and reviewing internal processes
- Managers – Responsible for implementing privacy procedures and policies, considering privacy issues and handling personal information across business units
- Front line staff – Comply with the privacy procedures and policies
- Human Resources – Responsible for training staff and inducting newly appointed individuals about the privacy policies and procedures
- Governance and Legal – Responsible for managing and ensuring legal compliance, providing advice and reporting about privacy obligations

3.6.2 Common Privacy Framework of the Information Privacy Commissioner of Ontario – CCIM Assessment Projects

The Community Care Information Management (CCIM) has developed a common privacy framework to guarantee that privacy practices are aligned with the requirements of the Information Privacy Commissioner of Ontario (IPC) (Community Care Information Management, 2010). While participating in CCIM assessment projects, health service providers (HSPs) have identified their clients' privacy concerns and adopted certain critical requirements when implementing electronic assessments.

The CCIM identified high-level requirements from the health service providers:

- Privacy awareness and training must be addressed.
- The need for privacy procedures and policies must be addressed.
- Consent management must be included to cover the lifecycle of the consent directive.
- Consent collection should be addressed, including the management, recording, communication and updating of the consent directive.
- The use of physical and electronic consent management/capture should be used.
- Incident and breach management should be supported.
- Public communication should be included.
- The framework should be flexible to support client privacy rights and accommodate existing policies.

The CCIM (Figure 3-3) consists of three layers, namely Privacy Governance, Privacy Policies and Procedures, and Privacy Operations.

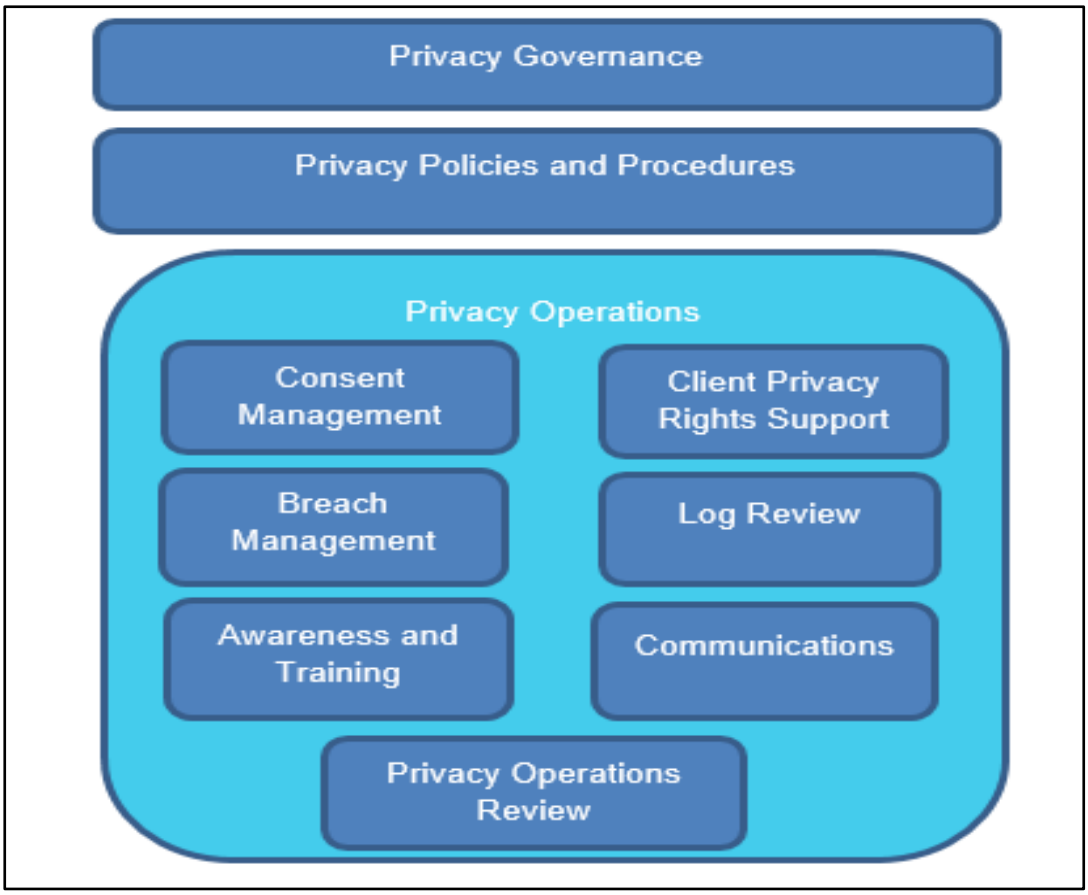


Figure 3-3: Common Privacy Framework (Community Care Information Management, 2010)

In Figure 3-3 above, the Privacy Governance layer provides the “privacy strategy and direction, and documents decisions on key privacy issues”. The next layer, the Privacy Policies and Procedures layer, “defines the specifications for privacy operations according to the direction and decisions from the Privacy Governance layer”. Lastly, the Privacy Operations layer addresses the “day-to-day privacy issues” that are defined by the processes of the Privacy Policies and Procedures layer.

Table 3-3: CCIM Privacy governance process

Framework	Description
Requirements	**Governance structure** – Senior management should appoint the Privacy Officer who may be part of the executive team or report directly to them. The Privacy Officer is responsible for all privacy-related matters.
	Governance process – Privacy strategy and direction are set by senior management with input from the Privacy Officer. Senior management should be committed to the success of the privacy strategy.
Design	**Establish privacy governance** – Establish privacy governance by formalising the appointment of the Privacy Officer who is accountable for privacy issues. The reporting structure of the Privacy Officer and his responsibilities and roles must be stated clearly.
	Set privacy strategy – This is based on legislative requirements, organisational culture, business objective, etc.
	Develop privacy policies and procedures – Specifications for operational activities and privacy management are defined.
	Oversee privacy management programme – Monitor or oversee the privacy management programme, including operational activities, and make appropriate improvements if privacy programme deviates from the privacy strategy.
Implementation	**People** – The Privacy Officer should be appointed by senior management and should ensure all staff are aware of his role and function.
	Process – Privacy governance should be integrated into the overall governance framework.
	Technology – Technology is not a requirement for the implementation of privacy governance.

Source: Community Care Information Management (2010)

Table 3-3 above describes the requirements, design and implementation process for the CCIM Privacy Governance Framework. The requirements phase includes the governance structure and process. The design phase includes the establishment of the privacy governance structure; it sets the privacy strategy, develops privacy policies and procedures, and lastly, oversees the privacy programme. The implementation phase describes the people who are part of the privacy role and function, the process for the implementation of privacy governance and lastly, technology.

3.6.3 Privacy Management Program – The Office of the Privacy Commissioner of Canada

In Canada, the Office of the Privacy Commissioner (OPC) and the offices of the Information and Privacy Commissioners (OIPCs) of Alberta and British Columbia have developed the Privacy Management Program to provide guidance for organisations to be accountable. This Privacy Management Program is based on the Canadian

Personal Information Protection and Electronic Documents Act (PIPEDA) (PIPEDA, 2015) which regulates privacy practices and the processing of personal information by organisations (Office of Privacy Commissioner, 2016). PIPEDA contains ten accountability or fair information principles to which organisations are expected to adhere to process and protect individuals' personal information (Office of Privacy Commissioner, 2016). While the framework is called a "Privacy Management Program" it was included in the scope as it focusses on the management of the program and not the program as such, and includes ongoing assessment and review in line with the definition of ISACA for privacy governance.

The Privacy Management Program (see Table 3-4) comprises two parts: Part A – Building Blocks, and Part B – Ongoing Assessment and Revision (Office of Privacy Commissioner, 2016). Table 3-5 portrays the components of the privacy governance framework, namely the Organisational Commitment, Program Controls, Oversight and Review Plan, and the Assess and Revise Program Controls as Necessary. The Organisational Commitment is further divided into the following sub-components namely: *Buy-in from the top*, *Privacy Officer*, *Privacy Office* and *Reporting*. The Program Controls component consists of the following sub-components: *Personal information inventory*, *Policies*, *Risk assessment tools*, *Training and education requirements, Breach and incident management response protocols*, *Service provider management* and lastly, *External communication*. The Oversight and Review Plan only consists of the *Development oversight and review plan* by the Privacy Officer. The *Assess and Revise Program Controls as Necessary* consists of all the sub-components of the Privacy Control component to assess and revise the programme controls.

Table 3-4: Privacy Management Program - The Office of the Privacy Commissioner of Canada

A. Building Blocks		
Organisational Commitment	a) Buy-in from the top	• Senior management support is vital to an effective privacy management programme and a privacy culture.
	b) Privacy Officer	• Important to business decision-making processes. • Monitors compliance roles and responsibilities which are recognised and conveyed throughout the organisation. • Responsible to develop and implement the programme controls and continuing assessment.
	c) Privacy Office	• Role and resources are identified. • Organisational structure supports employees to monitor compliance and promote a culture of privacy. • Ensures privacy protection is developed into every business function processing personal information.
	d) Reporting	• Organisation's programme controls need to reflect established reporting mechanisms.
Program Controls	a) Personal Information Inventory	The organisation must identify: • The personal information it controls and has in its possession. • Consent for the collection, disclosure and use of personal information and the sensitivity thereof.
	b) Policies	i. The disclosure and collection of personal information which include conditions for consent and notification ii. Accessibility and amendment of personal information iii. Personal information retention and disposal iv. Responsible use of information, including physical and technological security controls, and administrative and role-based access v. "Challenging compliance"
	c) Risk assessment tools d) Training and education requirements e) Breach and incident management response protocols f) Service provider management g) External communication	
B. Ongoing Assessment and Revision		
Oversight and Review Plan	a) Develop an oversight and review plan	An oversight and review plan must be developed by the Privacy Officer to monitor and assess the effectiveness of the privacy programme controls.
Assess and Revise Program Controls as Necessary	a) Update inventory of personal information. b) Review policies. c) Conduct risk assessment regularly. d) Modify training and awareness programmes. e) Adapt breach and incident response protocols. f) Conduct perfect service provider management. g) Improve external communication.	

Source: Office of Privacy Commissioner (2016)

3.6.4 The Office of the Australian Information Commissioner (OAIC) – Privacy Management Framework

The privacy management framework launched by the OAIC aims to assist federal public and private organisations to build a culture that promotes privacy protection in the organisation and adheres to privacy compliance on an ongoing basis (Segal, 2015).

The privacy management framework is based on the Australian Privacy Principle (APP) 1.2 (Office of the Australian Information Commissioner, 2015b). In terms of APP 1.2, an organisation must be proactive in implementing, maintaining and establishing privacy processes. To ensure compliance with APP, organisations must ensure the implementation of the required procedures, systems and practices (Office of the Australian Information Commissioner, 2015b). The framework proposes four steps to meet the ongoing compliance obligation and practise good privacy governance (Segal, 2015).

This framework was included as it incorporates the evaluation and monitoring of privacy requirements in line with the definition of privacy governance defined by ISACA although it is referred to as a management framework.

The four steps of the privacy management framework are as follows (Office of the Australian Information Commissioner, 2015b):

- Step 1: “Embed a culture of privacy that enables compliance” (Segal, 2015:296)
    - Personal information must be treated as a valuable asset to be protected, respected and managed.
    - Key roles and responsibilities must be appointed for privacy management.
    - Resources must be allocated for the implementation and development of a privacy management plan.
    - Reporting mechanisms must be implemented.
- Step 2: “Establish robust and effective privacy practices, procedures and systems” (Segal, 2015:296)
    - Privacy awareness must be promoted within the organisation.
    - Privacy risk across the organisation must be managed.

- Risk management processes must be implemented.
- Privacy enquiries must be handled.
- Complaints processes handling these matters must be established.
- The privacy policy must be updated regularly.

- Step 3: “Evaluate privacy practices, procedures and systems to ensure continued effectiveness” (Segal, 2015:297)
  - The privacy processes must be monitored and reviewed regularly.
  - The compliance of the privacy obligations, including privacy complaints, reviews and breaches, must be documented.
  - Performance against the privacy management plan must be evaluated regularly.
  - A feedback channel for employees and customers regarding privacy processes must be provided.
- Step 4 : “Enhance your response to privacy issues” (Segal, 2015:297)
  - Use step 3 evaluations to enhance the privacy processes.
  - Make use of external audits to identify areas of improvement.
  - The privacy implications, benefits and risks of new technologies must be examined and addressed.
  - Promote beneficial privacy standards, and introduce initiatives in your business practices.

3.6.5 Comparison of the privacy governance frameworks

Given the literature study and the selected privacy governance frameworks, a comparison table (Table 3-5) has been drafted to compare the components of the privacy governance frameworks. All the frameworks have the following components in common:

- Buy-in from the top
- Data Protection Officer/Office
- Reporting
- Policies
- Training and education requirements
- Breach handling/Incident management
- Oversight and review plan

Other components available in certain frameworks, but absent from others, are important, as they address privacy policies and processes applicable to organisations. Weber (2015) argues that there is no single solution for the protection of personal information and that a multifaceted approach is needed to encompass regulatory measures. There is, therefore, a gap that needs to be addressed to encompass all the components into a comprehensive framework.

A comprehensive privacy governance framework can thus be developed, by combining the components of the existing privacy governance frameworks discussed above. The comprehensive framework can serve as a strategic framework for the organisation by providing a privacy infrastructure to facilitate compliance, ongoing review processes and to promote a privacy culture (PCPD, 2014).

The components of the privacy governance frameworks listed in Table 3-5 are identified as all the components derived from the four privacy governance frameworks and the four literature articles discussed.

The components of each privacy governance framework and the literature articles are listed in the first column under the components heading of Table 3-5. In the top row, under the ‘Privacy Governance Framework’ heading, the frameworks that have been discussed in the literature are listed and the articles are listed under the column named ‘Literature articles’. The ‘x’ indicates that a component is included in the privacy governance framework and/or the literature articles. Each empty space in a framework column means that the component is not part of that framework or listed in the literature article. The total columns give an indication of how many frameworks have the same components in common and the ‘Total’ row gives an indication of how many of the components each framework has.

Table 3-5: Privacy governance framework comparison table

Components	**Privacy Governance Frameworks**				**Literature articles**				
	OIPC (Canada)	IPC North South Wales	CCIM - Ontario	OAIC - Australia	Herold (2005)	Delgado (2011)	Weber (2014	Seerden et al. (2018	Total (8)
1. Buy-in from the top	x	x	x	x		x	x		6
2. Data protection officer/office	x	x	x	x	x	x	x	x	8
3. Reporting	x	x	x	x	x				5
4. Personal data inventory	x			x	x	x	x	x	6
5. Policies	x	x	x	x	x	x	x	x	8
6. Risk assessment tools	x			x		x	x		4
7. Training and education requirements	x	x	x	x	x	x	x	x	8
8. Breach handling / Incident management	x	x	x	x	x	x	x	x	8
9. Communication	x	x	x						3
10. Data processor / Service provider management	x	x							2
11. Programme assurance /Audit			x	x	x	x			4
12. Oversight and review plan	x	x	x	x			x		5
13. Assess and revise programme controls	x	x		x			x		4
14. Promote the plan (Awareness)		x		x			x		3
Total (14)	12	11	9	12	7	8	10	5	

The OIPC and OAIC privacy frameworks each have 12 components of the 14 listed components in the table. The IPC North South Wales has 11 and the CCIM has nine components. For the literature articles, Herold (2005) has seven components, Delgado (2011) has eight, Weber (2014) has ten and Seerden et al. (2018) have five of the 14 components listed. According to the total components of the privacy governance framework, the OIPC Canada and OAIC Australia frameworks are the most comprehensive frameworks while the CCIM is the least comprehensive framework with only nine components.

Seerden et al. (2018) have the least components (5) for the articles. All four privacy governance frameworks and four articles have four components namely component two, five, seven and eight) in common.

3.7 Conceptual Framework for Privacy Governance

This section of the chapter will discuss the importance of a conceptual framework as well as the developing of the CPGF and its related components.

3.7.1 Importance of a conceptual framework

Miles and Huberman (1994:18) define a conceptual framework as “either graphically or in narrative form, the main things to be studied – the key factors, constructs or variables – and the presumed relationships among them”. A conceptual framework is primarily a model or conception of what needs to be studied (Maxwell, 2004). Maxwell (2004) states that a conceptual framework is something constructed and not merely founded. The conceptual framework of privacy governance is developed with components from various privacy governance frameworks in the literature studied, as Maxwell (2004) states that it is borrowed pieces that it incorporates but it is something that the researcher builds. The conceptual framework is, therefore, developed with components or modules when analysing the literature critically that ensures the components (Maxwell, 2004).

Maxwell discusses four sources for identifying the modules that are used when developing the conceptual framework, namely (Maxwell, 2004):

i. Your own experiential knowledge
ii. Thought experiments
iii. Existing theory and research
iv. Pilot and exploratory studies

For this study, the existing theory as a source is used to identify the important components for the conceptual framework for privacy governance. As per Maxwell (2004), the existing theory sheds light on phenomena and relationships, and lay outs data and their relationships with other data which can be depicted visually to display the conceptual framework.

3.7.2 Purpose of a privacy governance framework

The main purpose of a privacy governance framework is to ensure that privacy is adequately governed for the benefit of the organisation (Office of the Australian Information Commissioner, 2015b). According to the Office of the Australian Information Officer (2015), the objectives of the privacy governance framework are to embed a culture of privacy, establish effective and robust privacy processes, evaluate the privacy processes and enhance the response to privacy issues. With a solid privacy management programme in place, organisations will be able to strengthen good privacy practices, elevate the protection of personal information to a higher advanced level than prescribed in the legislative requirements, identify any weaknesses and demonstrate due diligence (Office of Privacy Commissioner, 2016).

The benefits of a privacy governance framework for the organisation are as follows (Office of the Australian Information Commissioner, 2015b):

i. It clarifies each person's role in the privacy governance programme.
ii. The privacy governance framework ensures accountability of each person.
iii. Once the policies, systems, processes and reporting structures are adequately and appropriately implemented, the privacy management will be integrated seamlessly into business-as-usual practices.
iv. A culture of privacy will be viewed as an asset and not as a liability among the staff of the organisation.

3.7.2.1 Negative impact of inadequate data privacy governance frameworks

When doing business with an organisation, individuals expect their personal information to be protected and their privacy to be respected by the company (AICPA, 2009). The American Institute of Certified Public Accountants (AICPA, 2009) identified eight specific risks when an organisation does not have an adequate privacy governance framework in place, namely:

i. The organisation's brand, business relationships and reputation can be damaged.
ii. Regulatory or industry sanctions and legal liability can be enforced against the company.

iii. The business can be charged for deceptive business practices.
iv. The company will experience employee or customer distrust.
v. Individuals will deny their consent for the company to process their personal information.
vi. Loss of market share and business revenue will occur.
vii. International business operations will be disrupted.
viii. The business will be liable for identity theft.

These risks should be considered when using a privacy governance framework to avoid any negative impact to the organisation as the responsible party or the individual as the data subject.

3.7.3 Components of the Conceptual Privacy Governance Framework

The proposed CPGF consists of four components, namely:

i. *Organisational Commitment*
ii. *Privacy Policies and Procedures*
iii. *Privacy Programme Controls*
iv. *Ongoing Assessment and Review*

Each component comprises the following sub-sections, namely *Leadership Commitment*; *Information Officer*; *Privacy Office*; *Reporting*; *Privacy Policies and Procedures*; *Personal Information Inventory*; *Service Provider Management*; *Breach Handling / Incident Management*; *Communication*; *Privacy Awareness and Training*; *Risk Assessment Tools*; *Programme Assurance / Audit*; and *Ongoing Assessments and Evaluation.* All the sections follow a top-down approach, from management to employees, to implement all the privacy structures, policies and procedures to ensure the protection of personal information.

Table 3-6 depicts the CPGF components derived from the theory, namely governance theory discussed in section 3.2, the literature review articles in section 3.4 and the four selected privacy governance frameworks from section 3.6. The one asterisk (*) represents components from the governance theory and the two asterisks (**)

represent components from the four privacy governance frameworks and literature articles in line with Table 3-5.

Table 3-6: Privacy governance framework components

Organisational Commitment	**Privacy Policies and Procedures**	**Privacy Programme Controls**	**Ongoing Assessment and Review**
* / ** Leadership Commitment	** Privacy Policies and Procedures	* / ** Personal Information Inventory	***** / ** Ongoing Assessments and Evaluation
** Information Officer		* / ** Breach Handling / Incident Management	
** Privacy Office		** Service Provider Management	
***** / ** Reporting		***** / ** Communication	
		** Privacy Awareness and Training	
		* / ** Risk Assessment Tools	
		***** / ** Programme Assurance / Audit	

Governance theory (section 3.2)

***** Selected privacy governance frameworks and literature articles (sections 3.4 and 3.6)***

The CPGF starts from Organisational Commitment which formulates the privacy objectives and strategy by the governing board. The Privacy Policies and Procedures are then developed by the senior managers of the organisation and then communicated to the privacy programme management section that implements the privacy programme controls. The Privacy Programme Controls are developed to ensure that the policies and procedures are implemented and are compliant with the privacy legislation (Office of Privacy Commissioner, 2016). The Ongoing Assessment and Review section of the framework assesses and reviews the privacy programme controls which are then communicated and reported to the privacy programme management and the shareholders of the organisation.

The effectiveness of the privacy programme or privacy breaches are reported to the relevant stakeholders. The audit reports are then reviewed by the Information Officer

and the governing body to revise the privacy policies and the procedures to ensure that the organisation is compliant with the privacy regulations and environmental changes. The CPGF is an ongoing process flow to ensure that the right policies and procedures are communicated to the relevant stakeholders and to promote a privacy culture among the employees.

Figure 3-4 presents a diagrammatic representation of Table 3-6 to indicate the cycle of the phases illustrating continuous improvement.

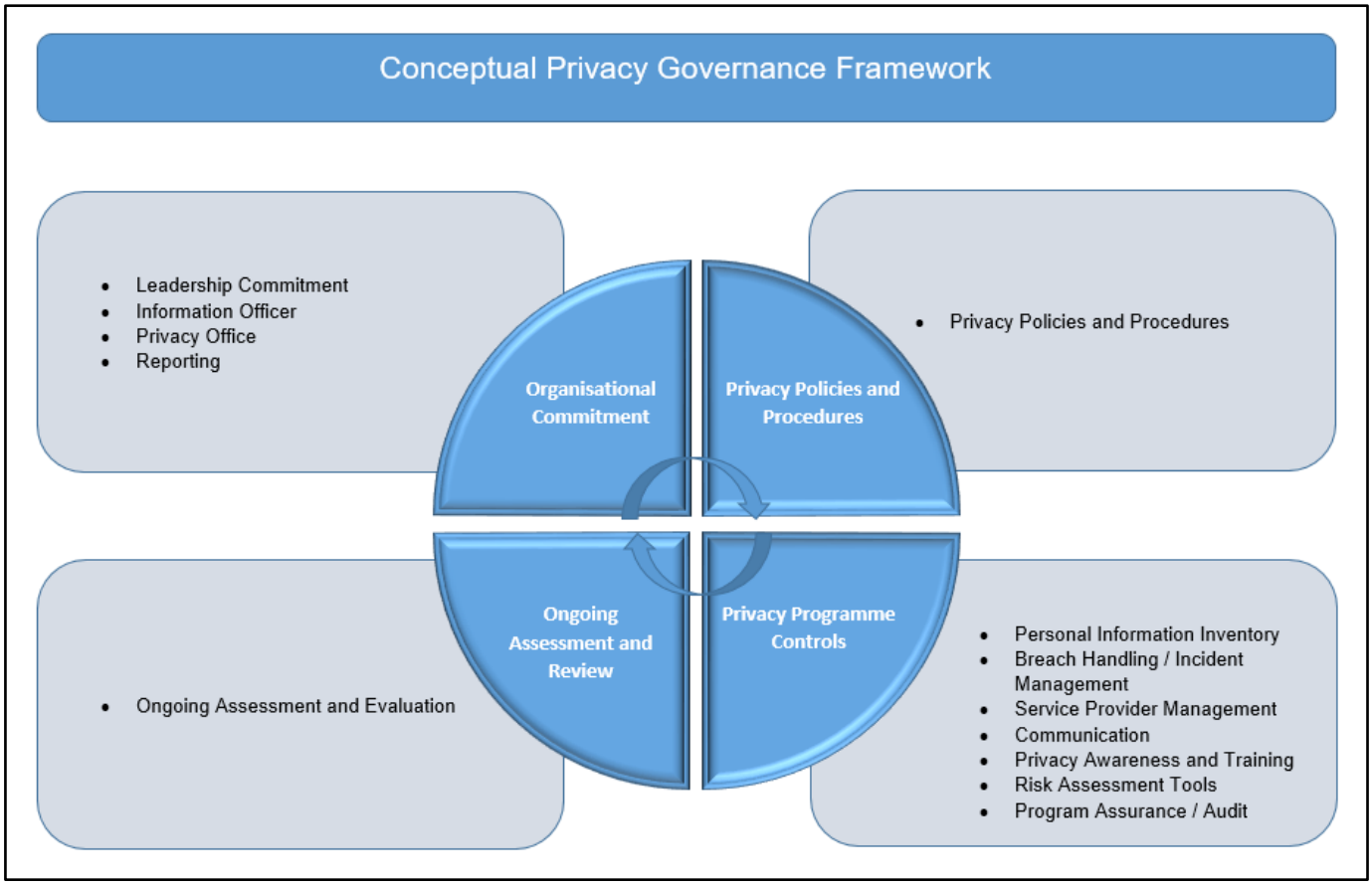


Figure 3-4: Conceptual Privacy Governance Framework

Table 3-7 below gives an overview of how the components of the CPGF map to the privacy governance framework comparison table (refer to Table 3-5). The numbers in column two, the “Reference no’s to Table 3-5” column, refer to the components represented under the “Components” column of Table 3-5. Each component of the CPGF in the “Components” column of Table 3-7 map to the components, which are numbered 1-14, in Table 3-5. Components 7 (*Training and education requirements*) and 14 (*Promote the plan [awareness]*) in Table 3-5 have been combined in one

component named as *Privacy awareness and training* in Table 3-7. The *oversight and review plan* (Table 3-5, no. 12) and *Assess and revise programme controls* (no. 13) have been combined in one subcomponent called "*Ongoing assessments and evaluation*". Both components 12 and 13 in Table 3-5 refer to the review and monitoring of the privacy programme controls.

Table 3-7 illustrates how the final components in the CPGF aligns with Table 3-5.

Table 3-7: Alignment of Conceptual Privacy Governance Framework based on Table 3-5 components

Components	**Reference no.'s to Table 3-5**
Leadership Commitment	1
Information Officer	2
Privacy Office	2
Reporting	3
Privacy Policies and Procedures	5
Personal Information Inventory	4
Breach Handling / Incident Management	8
Service Provider Management	10
Communication	9
Privacy Awareness and Training	7, 14
Risk Assessment Tools	6
Programme Assurance / Audit	11
Ongoing Assessments and Evaluation	12, 13

The next section gives an overview of each of the components of the CPGF. It provides the theoretical base for the privacy statements that will be developed for the IPGQ to address content validity. The sub-section components of the CPGF are used in section 3 of the IPGQ (Appendix G). The headings of section 3 of the questionnaire are the following: *Leadership Commitment*; *Information Officer*; *Privacy Office*; *Reporting*; *Privacy Policies and Procedures*; *Personal Information Inventory*; *Breach Handling / Incident Management, Service Provider Management*; *Communication*; *Privacy Awareness and Training*; *Risk Assessment Tools*; *Programme Assurance / Audit*; and *Ongoing Assessments and Evaluation.*

3.7.3.1 Organisational Commitment

Organisational commitment consists of the following components which are briefly discussed: Leadership Commitment, Information Officer, Privacy Office and Reporting.

Leadership Commitment

The first condition of the POPIA legislation is accountability which the organisation, as the responsible party, must act upon when processing personal information. To be accountable, the leadership (senior management) must be committed to ensure that the organisation is compliant with privacy legislation (Office of Privacy Commissioner, 2016).

The King IV Report highlights four roles and responsibilities of top management as the governing body, namely: (1) “Steers and sets strategic direction”; (2) “Approves policy and planning”; (3) “Oversees and monitors”; and (4) “Ensures accountability” (IODSA, 2016:40). From these responsibilities, it is indicated that the leadership of the organisation is responsible for setting the strategic direction for privacy (Bamberger & Mulligan, 2011), developing privacy policies, overseeing and monitoring the privacy program and ensuring accountability for privacy. These responsibilities are often implemented by appointing an Information Officer (POPIA, 2013), establishing a data Privacy Office and ensuring that privacy policies are in place that set the strategic direction (Office of Privacy Commissioner, 2016). The direction and commitment from the leadership will aid in establishing privacy across the organisation (Office of Privacy Commissioner, 2016). The implementation of privacy plans and guidelines by senior management ensure that employees embrace the seriousness of privacy (Bamberger & Mulligan, 2011).

The privacy programme is actively championed by senior management who should:

- Illustrate commitment from leadership (Community Care Information Management, 2010; Herold, 2005; Office of Privacy Commissioner, 2016; Office of the Australian Information Commissioner, 2015b).

- Set the privacy strategy and develop privacy policies and procedures in line with the privacy strategy (Bamberger & Mulligan, 2011; Community Care Information Management, 2010; Office of Privacy Commissioner, 2016).
- Implement privacy plans and guidelines (Bamberger & Mulligan, 2011; Herath, 2011; Office of Privacy Commissioner, 2016).
- Oversee the privacy programme (Herath & Rao, 2009; Herold, 2005; Office of Privacy Commissioner, 2016; Office of the Australian Information Commissioner, 2015b; Weber, 2015).

From the above theoretical statements, corresponding items can be defined that can be used in the IPGQ. Table 3-8 portrays the theoretical statements in column one with the corresponding item in column two.

Table 3-8: Theoretical statements of Leadership Commitment

Leadership Commitment	
Theoretical Statements	**Typical Items**
- Commitment from leadership	- ABC is committed to the protection of personal information.
- Set the privacy strategy and develop privacy policies and procedures in line with the privacy strategy.	- The privacy policies are in line with the privacy strategy.
- Implement privacy plans and guidelines.	- Management provides me with adequate guidance to implement the regulatory requirements of the Protection of Personal Information Act in my daily duties.
- Oversee the privacy programme.	- ABC has a function to effectively oversee the privacy programme.

Information Officer

Part B of Chapter 5 (Section 55) of the POPIA describes the responsibilities of an Information Officer and deputy Information Officer. The role of the Information Officer is very important for the strategic planning of the business as well as the assessment and revision of the privacy programme (Herath, 2011; Office of Privacy Commissioner, 2016; Office of the Australian Information Commissioner, 2015b). The position of the Information Officer should be filled by an individual with a strategic view of today's

privacy operations and tomorrow's planning (Herold, 2005). According to the Promotion of Access to Information Act (PAIA) of 2000, the Information Officer is the CEO or equivalent officer; therefore, the Information Officer is appointed by the CEO and should report directly to the CEO (PAIA, 2000).

Information Officers are, therefore, an integral component and assist with the privacy decision-making process (Bamberger & Mulligan, 2011). To promote the fulfilment of strong compliance standards and management commitment, privacy controls are developed and implemented (Bamberger & Mulligan, 2011). Information Officers also promote a privacy culture among employees and consistent privacy practices across the organisation (Bamberger & Mulligan, 2011). To achieve privacy goals, privacy controls are continuously assessed and revised by the Information Officer (Bamberger & Mulligan, 2011; Office of Privacy Commissioner, 2016).

According to the POPIA (2013), section 55, the responsibilities of the Information Officer are to:

- Encourage the organisation to comply with the lawful processing of personal information.
- Attend to requests made to the organisation in relation to the POPIA legislation.
- Collaborate with the Information Regulator regarding investigations that affect the organisation.

The key responsibilities and duties of the Information Officer, as summarised from the privacy governance frameworks and academic literature, include the following:

- Ensure compliance with the lawful processing of personal information (OIPC, 2016; POPIA, 2013).
- Assist with the business decision-making process (Bamberger & Mulligan, 2011; Herath, 2011; Office of Privacy Commissioner, 2016).
- Develop and implement privacy controls (Community Care Information Management, 2010; Herath, 2011; Office of Privacy Commissioner, 2016; Office of the Australian Information Commissioner, 2015b).

- Revise and assess the privacy controls continuously (Community Care Information Management, 2010; Herath, 2011; Office of Privacy Commissioner, 2016; Office of the Australian Information Commissioner, 2015b).
- Promote a privacy culture (Community Care Information Management, 2010; Herath, 2011; Office of Privacy Commissioner, 2016; Office of the Australian Information Commissioner, 2015b).

From the above theoretical statements, corresponding items can be defined that can be used in the privacy governance questionnaire. Table 3-9 portrays the theoretical statements in column one with the corresponding item in column two.

Table 3-9: Theoretical statements of an Information Officer

Information Officer	
Theoretical Statements	**Typical Items**
- Ensure compliance with the lawful processing of personal information.	- The Information Officer ensures compliance with the regulatory requirements of the Protection of Personal Information Act.
- Information Officer's role is important to assist with the business decision-making process.	- The Information Officer's role is effective to give input to business decision-making in ABC. - I know who the Information Officer in my organisation is.
- Develop and implement privacy controls.	- The Information Officer ensures that the privacy controls (e.g. training, audits, risk assessments, incident management) are implemented in ABC.
- Revise and assess the privacy controls continuously.	- The Information Officer effectively revises the privacy controls annually.
- Promote a privacy culture.	- The Information Officer effectively promotes a culture of privacy.

Privacy Office

The POPIA does not describe the functioning of the Privacy Office in detail but highlights the designation and delegation of the Information Officer and deputy Information Officer. According to the IAPP-EY report of 2018, a global mean of the numbers of employees who have worked full time in the organisation has increased

from 6.8 to 10 full-time privacy employees; therefore, it is necessary to establish a Privacy Office (Hughes & Saverice-Rohan, 2018). The Information Officer is the head of the Privacy Office to establish authority for privacy activities and accountability. The Information Officer, therefore, has the authority to implement changes and administer sanctions (Herold, 2005). The Privacy Office team usually consists of different team members of all areas of the organisation (Herold, 2005).

The main responsibilities of the Privacy Office, as identified by the IAPP-EY privacy governance survey, are the development of privacy policies and procedures, privacy training and awareness, privacy breach and incident management, the design and implementation of privacy controls, communication and privacy impact assessment (Hughes & Leizerov, 2016). The Privacy Office must ensure that privacy protection is built in every application and major function (Office of Privacy Commissioner, 2016). Resources need to be allocated to the Privacy Office to handle privacy queries and to promote privacy awareness within the organisation (Office of the Australian Information Commissioner, 2015b). Privacy issues and leading privacy practices must be communicated to senior management to help demonstrate due diligence and ensure an effective privacy program (Herold, 2005). When establishing the Privacy Office, the roles must be defined, and by identifying the resources, these must also be adequate (Office of Privacy Commissioner, 2016).

The following responsibilities/roles are important for the Privacy Office:

- Ensure that the protection of personal information is implemented in every procedural function or application (Herath, 2011; Office of Privacy Commissioner, 2016; Office of the Australian Information Commissioner, 2015c).
- Define the Privacy Office's role and provide resources (Community Care Information Management, 2010; Herath, 2011; Office of Privacy Commissioner, 2016; Office of the Australian Information Commissioner, 2015b).
- Routinely communicate privacy issues to senior management (Community Care Information Management, 2010; Herold, 2005; Office of Privacy Commissioner, 2016; Office of the Australian Information Commissioner, 2015b).

Table 3-10: Theoretical statement of Privacy Office

Privacy Office	
Theoretical Statements	**Typical Items**
- Ensure that the protection of personal information is implemented in every procedural function or application.	- The Privacy Office effectively manages the protection of personal information in every major function. - I am aware of the privacy controls in the application/s that I am using. - I am aware of the privacy controls in the procedural functions that I have to follow.
- Define Privacy Office's role and provide resources.	- I am aware of the role of the Privacy Office. - The resources of the Privacy Office are effective in promoting privacy awareness.
- Routinely communicate privacy issues to senior management.	- My business unit has a clear reporting line to the Privacy Office.

Reporting

According to the King IV Report, the governing body needs to report to stakeholders in a meaningful and transparent manner (King IV Report, 2016). Principle 5 of the King IV Report states that the reports issued by the governing body of the organisation help the stakeholders to make informed assessments (King IV Report, 2016), and also demonstrate that the organisation complies (PCPD, 2014) with the relevant laws. Compliance with privacy laws, privacy commitments (e.g. publicly displayed privacy promises or individual commitments [Teltzrow & Kobsa, 2004]), policies and procedures and service-level agreements is reviewed and documented (AICPA/CICA, 2011).

The outcome of the reviews should be reported to senior management (AICPA/CICA, 2011). The IAPP-EY 2016 survey shows that 6% more organisations have used internal audits compared to the previous year to perform privacy audits within the organisations and to report the findings to senior management (Hughes & Leizerov, 2016). Within large organisations, the outcomes of the investigations and audits conducted by third-party verification institutes in regard to compliance with local privacy laws are reviewed and reported to senior management (AICPA/CICA, 2011; Office of Privacy Commissioner, 2016).

For an effective reporting programme, all the reporting structures need to be documented, reporting structures must be clearly defined and a test run needs to be performed on the internal reporting structures (Office of Privacy Commissioner, 2016; PCPD, 2014). Escalation procedures must be documented and communicated to all employees of the organisation to report a privacy issue or breach (Community Care Information Management, 2010; Office of Privacy Commissioner, 2016).

The Reporting component includes the following aspects:

- All reporting structures must be documented (Office of Privacy Commissioner, 2016; Office of the Australian Information Commissioner, 2015b).
- The reporting structures must be clearly defined (Office of Privacy Commissioner, 2016; Office of the Australian Information Commissioner, 2015b).
- Escalation reporting structures for employees must be in place to report any privacy issues (Community Care Information Management, 2010; Office of Privacy Commissioner, 2016).

From the above theoretical statements, corresponding items can be defined that can be used in the IPGQ. Table 3-11 portrays the theoretical statements in column one with the corresponding item in column two.

Table 3-11: Theoretical statements of Reporting

Reporting	
Theoretical Statements	**Typical Items**
- All reporting structures must be documented.	- My department receives privacy reports annually. - The privacy reports are comprehensive enough to develop remediation plans.
- The reporting structures must be clearly defined in the privacy programme controls.	- I am aware of the contents of the privacy compliance report. - I believe I should receive the privacy report that affects my daily duties.
- Escalation reporting structures for employees must be in place to report any privacy issues.	- I am aware of the escalation process in ABC to report any privacy issue.

3.7.3.2 Privacy Policies and Procedures

Privacy Policies and Procedures

Privacy policies must be documented and developed in accordance with Condition 8 of the POPIA, 2013 (PCPD, 2014; POPIA, 2013). Policies and operational plans are developed by management who gives direction with regard to privacy strategies according to the King IV Report, and must be approved by the governing body (King IV Report, 2016). The privacy policy provides operational support to the employees of the organisation for the protection of personal information (Herath, 2011). Senior management decides on the specifications for the privacy operations according to the definitions of the privacy policies and procedures (Community Care Information Management, 2010). It is important that the privacy policies are aligned with the business processes and procedures (Dennedy et al., 2014).

Privacy policies must further be developed so that they give effect to the privacy principles contained in the privacy legislation (Office of Privacy Commissioner, 2016). The privacy controls must address the handling of personal information throughout the information lifecycle and also clearly document how employees must handle personal information in their everyday duties (Office of the Australian Information Commissioner, 2015b). A privacy policy, therefore, provides direction on privacy practices (Community Care Information Management, 2010). Privacy procedures are the end product of what is established in one or more policies (Community Care Information Management, 2010).

The following key aspects of Privacy Policies and Procedures are essential for organisations:

- Organisations must have privacy policies in place (Community Care Information Management, 2010; Herath, 2011; Office of the Australian Information Commissioner, 2015b; POPIA, 2013; Weber, 2014).
- Privacy policies must be developed so as to give effect to the privacy principles contained in the privacy legislation (Community Care Information Management, 2010; Office of Privacy Commissioner, 2016).
- Privacy policies must be aligned with business processes and procedures (Dennedy et al., 2014; Herath, 2011; Office of Privacy Commissioner, 2016).

- A privacy policy with clear direction on the procedures and standards for the protection of personal information must be developed (Community Care Information Management, 2010; Herath, 2011; Office of Privacy Commissioner, 2016).

From the above theoretical statements, corresponding items can be defined that can be used in the IPGQ. Table 3-12 portrays the theoretical statements in column one with the corresponding item in column two.

Table 3-12: Theoretical statements of Privacy Policies and Procedures

Privacy Policies and Procedures	
Theoretical Statements	**Typical Items**
- Organisations must have privacy policies in place.	- The privacy policy is understandable. - The privacy statement on the ABC website is understandable.
- Privacy policies that give effect to the privacy principles contained in the privacy legislation must be developed.	- The privacy policy assists me with the implementation of privacy controls in my daily duties.
- Privacy principles must be clearly defined in the privacy policy.	- The privacy principles I follow in my daily duties are clearly defined in the privacy policies.
- Privacy policies must be aligned with business processes and procedures.	- The business processes and procedures are supported by the privacy policy.
- A privacy policy with clear direction for the privacy procedures and standards to protect personal information must be developed.	- There are clear privacy standards and procedures in our business unit.

3.7.3.3 Privacy Programme Controls

The privacy programme controls are briefly discussed below. They are *Personal Information Inventory, Breach Handling / Incident Management, Service Provider management, Communication, Privacy Awareness and Training, Risk Assessment Tools and Programme Assurance/Audit*.

Personal Information Inventory

Condition 3 of the POPIA portrays the purpose for the processing, retention and restriction of records by the responsible party. The organisation, therefore, has to keep an inventory of the personal information records it processes, according to a survey done by IAPP-EY 2016 (Hughes & Leizerov, 2016). Personal information collected

should also be documented as well as the reason for processing the personal information (ISO/EIC, 2011).

There are two types of information, namely personal information (e.g. name, identity number, telephone number, etc.) and sensitive personal information (e.g. religious belief, race, political beliefs, etc.) (Office of the Australian Information Commissioner, 2015b). The POPIA refers to sensitive personal information as special personal information under Condition 8 section 26-33. It states that special personal information must not be processed by the responsible party without the consent of the data subject, a court order or compliance with international public law (POPIA, 2013). Organisations must document and understand the personal information they process and where it is stored (Office of Privacy Commissioner, 2016). This understanding of personal information will enable the organisations to protect the personal information, obtain the correct type of consent (Community Care Information Management, 2010) and assist the data subject to exercise his or her access and correction rights (Office of Privacy Commissioner, 2016).

The importance of Personal Information Inventory is to:

- Identify the personal information the organisation processes (Community Care Information Management, 2010; Office of Privacy Commissioner, 2016).
- Determine the sensitivity of the personal information (AICPA/CICA, 2011; Community Care Information Management, 2010; Office of Privacy Commissioner, 2016).
- Document the reason for collecting and processing personal information (AICPA/CICA, 2011; ISO/EIC, 2011; Office of Privacy Commissioner, 2016; POPIA, 2013).

From the above theoretical statements, corresponding items can be defined that can be used in the IPGQ. Table 3-13 portrays the theoretical statements in column one with the corresponding item in column two.

Table 3-13: Theoretical statements of personal information inventory

Personal Information Inventory	
Theoretical Statements	**Typical Items**
- Identify the personal information the organisation processes.	- I know how to identify personal information.
- Determine the sensitivity of the personal information.	- I know how to identify sensitive personal information.
- Document the reason for collecting and processing personal information.	- Personal information collected by ABC is relevant for my daily tasks. - Reasons for the collecting and processing of personal information are documented.

Breach Handling / Incident Management

Section 22 (Condition 7) of the POPIA states that if there is a breach of personal information, the Information Regulator and data subject need to be informed of such incident. Policy, duty, contract or procedure infringement could be the cause of an incident which will expose sensitive personal information to unauthorised parties (Community Care Information Management, 2010). Therefore, privacy breaches and security incidents can occur due to unauthorised access to data, negligence of employees or malicious and criminal attacks (Da Veiga & Martins, 2015). Privacy breaches, therefore, have a negative impact on organisations, e.g. legal penalties, fines, loss of revenue and brand damage (Herold, 2005). A procedure that handles personal information incidents must be in place to ensure that the organisation takes remedial action swiftly and also to prevent such incidents from reoccurring (PCPD, 2014). A breach-handling procedure must be clearly documented and needs to be followed in the breach/incident management control, namely detection, escalation, breach handling, breach notification and reporting (Community Care Information Management, 2010). When a breach is reported, it should include the corrective actions, remedial procedures and lessons learned (Community Care Information Management, 2010). Privacy breaches must be reported in a timely manner and to the appropriate channels (AICPA, 2009).

The important aspects of the Breach Handling / Incident Management are:

- Breach-handling procedures must be clearly documented and include five activities, namely detection, escalation, breach handling, breach notification and reporting (AICPA/CICA, 2011; Community Care Information Management, 2010; Office of Privacy Commissioner, 2016; POPIA, 2013).
- The negative impact of privacy breaches on organisations should be understood (Community Care Information Management, 2010; Herath, 2011; Herold, 2005).
- If a breach is detected, it should be reported and logged, and should include the corrective actions, resolution and lessons learned (AICPA/CICA, 2011; Community Care Information Management, 2010; Office of Privacy Commissioner, 2016).

From the above theoretical statements, corresponding items can be defined that can be used in the IPGQ. Table 3-14 portrays the theoretical statements in column one with the corresponding item in column two.

Table 3-14: Theoretical statements of Breach Handling / Incident Management

Breach Handling / Incident Management	
Theoretical Statements	**Typical Items**
- Breach-handling procedures must be clearly documented and include five activities, namely detection, escalation, breach handling, breach notification and reporting.	- The privacy procedures are effective to prevent a privacy breach or incident. - I'm aware of the incident management procedure in ABC to report a privacy incident. - I'm aware of the breach handling procedure in ABC to report a privacy incident.
- The negative impact of privacy breach on organisations should be understood.	- I am aware of the consequences of the violation of privacy policies and procedures. - I am aware of the harmful effects (e.g. ABC brand and reputational damage, loss of market share and revenue, customer distrust and legal action against the company) of the violation of privacy policies and procedures.
- If a breach is detected, it should be reported and logged, and should include the corrective actions, resolution and lessons learned.	- The breach handling / incident management process of ABC is effective in resolving privacy incidents.

Service Provider Management

Condition 7, Section 21 of the POPIA of 2013 stipulates that a written contract between a service provider and the responsible party must be in place to ensure that the service provider or third party processes personal information lawfully and maintains the security measures (POPIA, 2013). Audits are conducted by the responsible party or external auditor to evaluate the third party (AICPA, 2009). This is supported by the GAAP principles (AICPA, 2009) that state that there must be service-level agreements in place with the organisation to protect the data subjects' personal information in line with the organisation's privacy policies and other requirements. Therefore, organisations have third-party contracts in place to ensure third parties comply with the contractual agreements and privacy requirements of the organisation (AICPA/CICA, 2011). However, third parties must be provided with guidelines; therefore, policies and procedures must be in place determining how the third parties will process the personal information and the premises where it will be processed (Office of Privacy Commissioner, 2016). To assist third parties to efficiently implement policy requirements it is important that their employees undergo training and audits be conducted on a regular basis (Office of Privacy Commissioner, 2016).

Privacy requirements for Service Provider Management, should include:

- Third-party agreements (written contracts) and audits must be in place to ensure compliance with the organisation's privacy policies and procedures (Herath, 2011; OIPC, 2016; POPIA, 2013).
- The service provider must comply with the service-level agreement or contract which includes adherence to the organisation's privacy policies (Herath, 2011; Office of Privacy Commissioner, 2016).
- Training and education for the service provider should be in place (Herath, 2011; Office of Privacy Commissioner, 2016).

From the above theoretical statements, corresponding items can be defined that can be used in the IPGQ. Table 3-15 portrays the theoretical statements in column one with the corresponding item in column two.

Table 3-15: Theoretical statements of Service Provider Management

Service Provider Management	
Theoretical Statements	**Typical Items**
- Third-party agreements and audits must be in place to ensure compliance with the organisation's privacy policies and procedures.	- Audits are conducted effectively to ensure that the service providers are compliant with ABC's privacy requirements as stipulated in the third-party contract. - A third-party contract is in place between ABC and all service providers.
- The service provider must comply with the service-level agreement or contract which includes adherence to the organisation's privacy policies.	- Service providers adhere to the privacy requirements in the third-party contract of ABC.
- Training and education for service providers should be in place.	- Data-privacy training for service providers is effective.

Communication

Condition 6 of the POPIA of 2013 requires the responsible party to be open and transparent. According to the POPIA (2013), the responsible party must inform the data subject regarding the collection of and/or purpose for altering or accessing his or her personal information as well as his or her rights if this is done. This is supported by the GAAP principles (AICPA, 2009) that state that communication to individuals, describing the criteria to communicate the personal information the organisation processes, accessing procedures to review, updating or correcting the information and revealing to whom the information is disclosed (AICPA/CICA, 2011). Therefore, organisations have a responsibility to inform the individuals of their privacy rights (Office of Privacy Commissioner, 2016; Office of the Australian Information Commissioner, 2015b) by means of privacy notices on their websites, social media and in mobile communication (AICPA/CICA, 2011). A privacy notice, according to the GAAP principle, must notify the data subject of the organisation's privacy policies and procedures as well as the collection, consent, purpose, use and disclosure of personal information (AICPA/CICA, 2011).

The data subject also has the right to be informed if his or her personal information has been accessed or acquired by an unauthorised person and may only be delayed if the incident is under investigation by a public body or the Information Regulator (POPIA, 2013). This communication to individuals about their rights to be informed

about the privacy policies and procedures implemented by the organisation must be clear and understandable (PCPD, 2014).

A privacy procedure must be in place to handle privacy-related complaints, inquiries, comments, questions or disputes according to the monitoring and enforcement principle of GAAP (AICPA/CICA, 2011). Changes in privacy policies or procedures affecting the processing of employees' personal information must be communicated to them as soon as senior management has modified the privacy policy (AICPA/CICA, 2011).

The important aspects of Communication are:

- The data subject must be provided with complete information regarding the collection, purpose, use and disclosure of his or her personal information (privacy rights) (AICPA/CICA, 2011; Community Care Information Management, 2010; Office of Privacy Commissioner, 2016; POPIA, 2013).
- A privacy notice should be placed on the organisation's website, informing the client about the privacy policies of the relevant organisation (AICPA/CICA, 2011; Community Care Information Management, 2010; Office of Privacy Commissioner, 2016).
- An individual must be notified if his or her personal information has been compromised (AICPA/CICA, 2011; Community Care Information Management, 2010; POPIA, 2013).
- Essential information must be communicated to employees who are impacted if there are changes made to the privacy policies or procedures of the organisation (Community Care Information Management, 2010; Herath, 2011; Office of Privacy Commissioner, 2016).
- Privacy communication must be clear and understandable (AICPA/CICA, 2011).

From the above theoretical statements, corresponding items can be defined that can be used in the IPGQ. Table 3-16 portrays the theoretical statements in column one with the corresponding item in column two.

Table 3-16: Theoretical statements of Communication

Communication	
Theoretical Statements	**Typical Items**
- Inform the data subject with complete information regarding the collection, purpose, use and disclosure of personal information.	- I have been informed about my privacy rights by ABC. - ABC has communicated the purpose for collecting the personal information to the staff.
- A privacy notice should be placed on the organisation's website informing the client about the privacy policies.	- I have read the privacy notice on ABC's website.
- An individual must be notified if his or her personal information has been compromised.	- ABC will notify me if my personal information has been compromised.
- Essential information must be communicated to employees who are impacted if there are changes made to the privacy policies or procedures.	- My colleagues are aware of privacy changes that affect their daily duties.
- Privacy communication must be clear and understandable.	- I have a clear understanding of all privacy communications.

Privacy Awareness and Training

According to the IAPP-EY survey of 2018, 90% of the respondents have indicated that training and awareness are two of the top privacy responsibilities. This finding indicates that organisations are committed to equip their employees with privacy training and skills through privacy policies and procedures (Hughes & Saverice-Rohan, 2018). Therefore, privacy awareness and training for employees are very important aspects to identify privacy breaches or to equip employees with skills to protect personal information (Office of Privacy Commissioner, 2016). However, privacy education and training need to be tailored for employees who work with personal information directly. This kind of training and education must be included in the induction programmes for new employees (AICPA/CICA, 2011; Office of Privacy Commissioner, 2016; Office of the Australian Information Commissioner, 2015b). Privacy training must train employees in understanding the relevant policies and procedures (AICPA, 2009). Privacy training must also be conducted annually to assess the employees' understanding as well as to update employees on any new changes to the privacy policies and procedures (AICPA/CICA, 2011; Office of the Australian Information Commissioner, 2015b). Privacy training must also be

mandatory before personal information is accessed (Office of Privacy Commissioner, 2016).

The important aspects of the Privacy Training and Awareness are:

- Privacy training must form part of the induction programme of new employees (Community Care Information Management, 2010; Office of Privacy Commissioner, 2016; Office of the Australian Information Commissioner, 2015b).
- The privacy training must be developed in line with the privacy policies and procedures (Community Care Information Management, 2010; Office of Privacy Commissioner, 2016; Office of the Australian Information Commissioner, 2015b).
- Privacy training must be mandatory and accessible for all employees before personal information is processed (Community Care Information Management, 2010; Office of Privacy Commissioner, 2016; Office of the Australian Information Commissioner, 2015b).
- Annual training or refresher training is necessary to address new privacy policies (Community Care Information Management, 2010; Office of Privacy Commissioner, 2016; Office of the Australian Information Commissioner, 2015b).

From the above theoretical statements, corresponding items can be defined that can be used in the IPGQ. Table 3-17 portrays the theoretical statements in column one with the corresponding item in column two.

Table 3-17: Theoretical statements of Privacy Awareness and Training

Privacy Awareness and Training	
Theoretical Statements	**Typical Items**
- Privacy training must form part of the induction programme of new employees.	- Newly appointed colleagues are provided with privacy training.
- The privacy training must be developed in line with the privacy policies and procedures.	- Privacy training is customised for my job role. - Privacy training equips my colleagues to implement the privacy policy.
- The privacy training must be mandatory and accessible for all employees before personal information is processed.	- I have completed the mandatory privacy compliance test.
- Annual training or refresher training is necessary to address new privacy policies.	- The privacy compliance test covers changes to the privacy policies.

Risk Assessment Tools

Condition 7 (section 19) of the POPIA of 2013 indicates that the responsible party must have measures in place to identify external and internal risks when processing personal information (POPIA, 2013). The criteria of the GAAP principles (AICPA, 2009) use risk assessment to establish a risk baseline, to identify new or changed risks to personal information and to update the responses to such risks (AICPA/CICA, 2011). Privacy-impact assessments can assist organisations with mitigating and identifying security risks and leakages (PCPD, 2014). Security controls implemented must be established and maintained to ensure that the safeguards are implemented and that they are updated regularly when new risks are identified (POPIA, 2013). Privacy-related problems can be prevented if proper risk assessment tools are in place; therefore, privacy risk assessments need to be conducted at least on an annual basis (Office of Privacy Commissioner, 2016).

Important aspects of the Risk Assessment Tools are as follows:

- Privacy risk assessments must be conducted to identify privacy risks (AICPA/CICA, 2011; Community Care Information Management, 2010; Office of Privacy Commissioner, 2016; POPIA, 2013).
- Risk assessment should be implemented to identify new or changed risks to personal information (AICPA/CICA, 2011; Community Care Information Management, 2010; Herath, 2011; Office of Privacy Commissioner, 2016).

- Risk assessment procedures must be in place to assess, identify and manage the privacy risk (AICPA/CICA, 2011; Community Care Information Management, 2010; Office of Privacy Commissioner, 2016; POPIA, 2013).

From the above theoretical statements, corresponding items can be defined that can be used in the IPGQ. Table 3-18 portrays the theoretical statements in column one with the corresponding item in column two.

Table 3-18: Theoretical statements of Risk Assessment Tools

Risk Assessment Tools	
Theoretical Statements	**Typical Items**
- Risk assessments must be conducted to identify privacy risks.	- ABC's privacy risk assessments are performed regularly.
- Risk assessment should be implemented to identify new or changed risks to personal information.	- New processes or systems are assessed for any potential privacy risk.
- Risk assessment procedures must be in place to assess, identify and manage the privacy risk.	- Privacy risks of existing processes are reviewed. - ABC's risk assessments help identify privacy risks.

Programme Assurance / Audit

Privacy assurance promotes customer trust when interacting with the organisation's website. Privacy assurance is defined as a statement supplied by the organisation on its website that the consumer's privacy is assured (Lowry, Moody, Vance, Jensen, Jenkins & Wells, 2012). Privacy assurance, such as privacy seals (e.g. TRUSTe and BBBOnline) and privacy statements promote customer disclosure of personal information, and customers can make accurate assessments of the risks when disclosing personal information (Bamberger & Mulligan, 2011; Hui, Teo & Lee, 2007). Such assurance programmes and audits will ensure compliance with the privacy policies (Office of Privacy Commissioner, 2016). Therefore, to improve the privacy processes, internal audits need to be conducted to identify areas of improvement (Office of Privacy Commissioner, 2016) as well as privacy self-assessments which are conducted by the business units (Da Veiga & Martins, 2015).

Proactive privacy audits are conducted by the organisation to protect personal information without it being requested by external agencies, and reactive privacy audits are conducted to ensure that privacy policies and procedures conform to internal rules and external requirements (Tancock, Pearson & Charlesworth, 2013). Following assessments and audits, policies are reviewed and revised in response to complaints, privacy breaches, and new guidance as a result of industry-based best practices (Office of Privacy Commissioner, 2016).

The following aspects are important for Programme Assurance / Audit control:

- Ensure that internal and external audits are conducted to monitor compliance with the privacy policies (Office of Privacy Commissioner, 2016; Office of the Australian Information Commissioner, 2015a).
- Rectify non-compliance or weaknesses of privacy policies and standards reviewed by the audit report (Office of Privacy Commissioner, 2016; Office of the Australian Information Commissioner, 2015a).
- Conduct privacy self-assessments (Office of Privacy Commissioner, 2016; Office of the Australian Information Commissioner, 2015a).

From the above theoretical statements, corresponding items can be defined that can be used in the IPGQ. Table 3-19 portrays the theoretical statements in column one with the corresponding item in column two.

Table 3-19: Theoretical statements of Programme Assurance / Audit

Programme Assurance / Audit	
Theoretical Statements	**Typical Items**
- Ensure that internal and external audits are conducted to monitor compliance with the privacy policies.	- Privacy audits are effectively conducted to monitor the compliance of privacy policies and procedures.
- Rectify non-compliance or weaknesses of privacy policies and standards reviewed by the audit report.	- Weaknesses or non-compliance with the privacy policies is revised.
- Conduct privacy self-assessments.	- Privacy self-assessments adequately prepares my department to be privacy compliant. - The Privacy Office effectively prepares my division for privacy audits.

3.7.3.4 Ongoing Assessment and Revision

The Ongoing Assessment and Revision are briefly discussed below, namely: *Oversight and Review Plan*, and *Evaluate Privacy Practices*.

Oversight and Review Plan

An oversight and review plan must be implemented by the privacy officer to ensure that the privacy management programme is monitored and assessed effectively (Office of Privacy Commissioner, 2016). As part of the strategic planning, the privacy officer should develop an oversight and review plan annually, and must include a schedule of when the privacy policies and controls will be reviewed (Office of Privacy Commissioner, 2016). Performance measures and a schedule of when all the privacy practices will be reviewed should be established (Office of Privacy Commissioner, 2016). The objective of the review plan ensures that the privacy operations are executed in alignment with the defined privacy processes (Community Care Information Management, 2010). This plan will assist senior management to assess and monitor the effectiveness of the organisation's privacy policies and practices (Office of Privacy Commissioner, 2016). Therefore the review report, presented to senior management, will include the risk rating, recommendations and the impact the risk will have on the business (Community Care Information Management, 2010).

The following aspects is important for the Oversight and Review Plan:

- The results of the privacy audits or self-assessments must be clearly documented and must include the risk rating, impact and recommendations (Community Care Information Management, 2010; Office of Privacy Commissioner, 2016; Office of the Australian Information Commissioner, 2015b).
- Establish performance measures and a schedule of when all the privacy practices will be reviewed (Community Care Information Management, 2010; Office of Privacy Commissioner, 2016; Office of the Australian Information Commissioner, 2015b).
- Review the implementation of the privacy governance framework and the progress in line with the strategic goals, privacy policies and practices (Community Care Information Management, 2010; Office of Privacy

Commissioner, 2016; Office of the Australian Information Commissioner, 2015b).

From the above theoretical statements, corresponding items can be defined that can be used in the privacy governance questionnaire. Table 3.20 portrays the theoretical statements in column one with the corresponding item in column two.

Table 3-20: Theoretical statements of Oversight and Review Plan

Oversight and Review Plan	
Theoretical statements	**Typical Items**
- The results of the privacy audits or self-assessments must be clearly documented and must include the risk rating, impact and recommendations.	- Privacy is monitored effectively within my organisation. - The recommendations of the privacy review plan are adequate.
- Establish performance measures should be and a schedule of when all the privacy practices will be reviewed.	- My business unit receives updates on the privacy review schedule.
- Review the implementation of the privacy governance framework and the progress towards your strategic goals, privacy policies and practices regularly.	- Privacy policies are reviewed for new technological advancements and systems.

Evaluate Privacy Practices

Privacy processes of organisations need to be improved on a continuous basis to ensure they are responsive and agile to new privacy issues (Segal, 2015). The various privacy programme controls must be assessed and reviewed on a regular basis. These controls are the *Personal Information Inventory, Breach Handling / Incident Management, Service Provider Management, Communication, Privacy Awareness and Training, Risk Assessment Tools, Programme Assurance / Audit* (Office of Privacy Commissioner, 2016). Therefore organisations must be informed of developments in privacy law; monitor and address privacy threats and risks; and lastly examine and address the privacy implications and benefits of new technologies (Segal, 2015). The effectiveness and appropriateness of the privacy practices should be systematically examined (Segal, 2015). Security, privacy issues and privacy practices should be effectively communicated to all personnel, managers and business partners (Herold, 2005).

The following aspects to Evaluate Privacy Practices are important:

- Review and update privacy controls to be effective to protect personal information (AICPA/CICA, 2011; Community Care Information Management, 2010; POPIA, 2013).
- Align privacy policies and procedures with new privacy developments and technological changes (Herath, 2011; Office of Privacy Commissioner, 2016; Office of the Australian Information Commissioner, 2015b).
- Receives communications of updated privacy practices (Herold, 2005; Office of Privacy Commissioner, 2016).

From the above theoretical statements, corresponding items can be defined that can be used in the privacy governance questionnaire. Table 3.21 portrays the theoretical statements in column one with the corresponding item in column two.

Table 3-21: Theoretical statements of Evaluate Privacy Practices

Evaluate Privacy Practices	
Theoretical statements	**Typical Items**
- Review and update privacy controls to be effective to protect personal information.	- Privacy controls (e.g. secure print, end-point protection, disk encryption, etc.) are evaluated.
- Align privacy policies and procedures with new privacy developments and technological changes.	- Privacy policies and procedures are updated regularly with technological changes.
- Receives communications of updated privacy practices.	- My business unit regularly receives privacy practice updates.

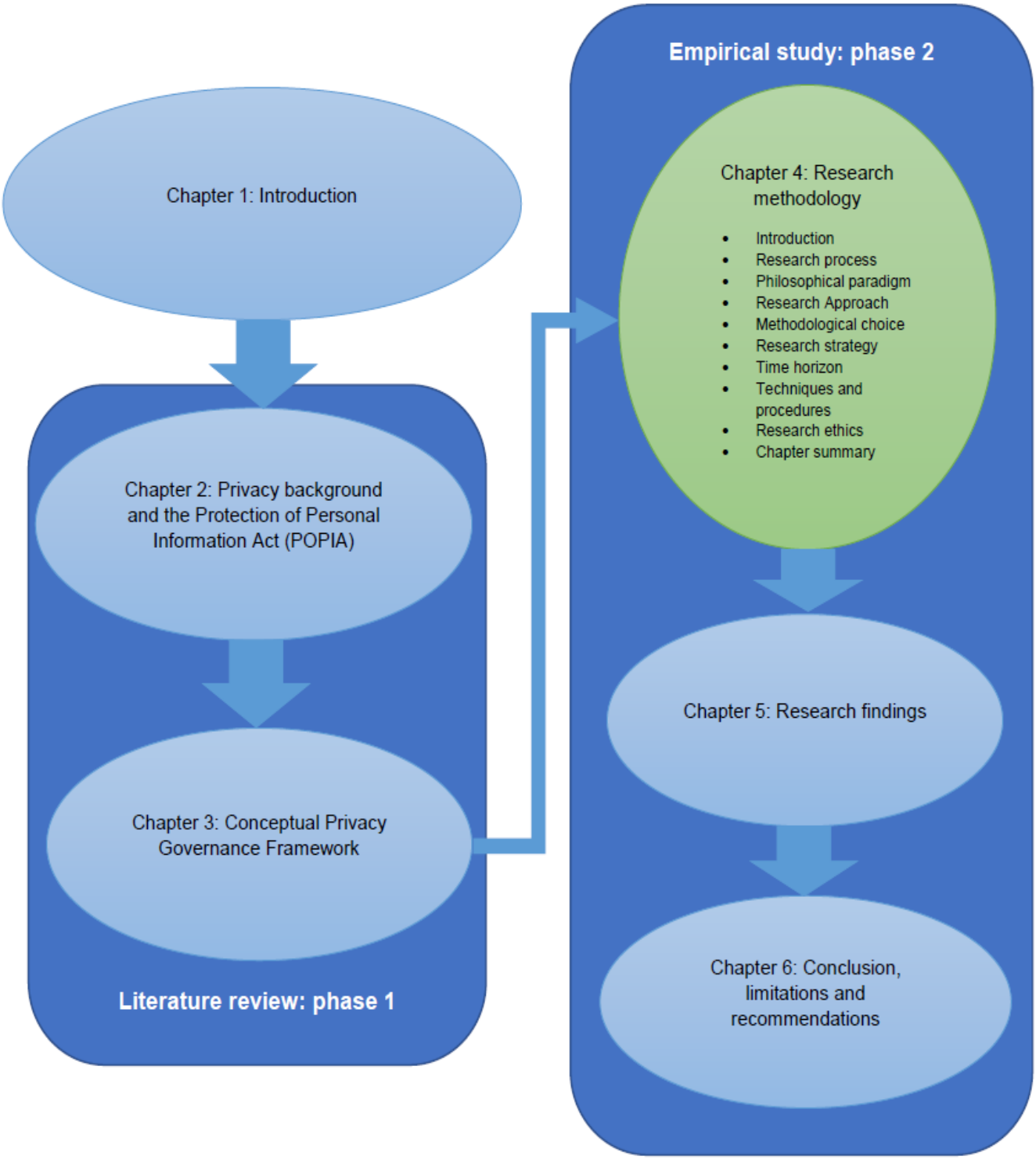
3.8 Chapter summary

The meaning of governance, which is the manner in which or action according to which an organisation is governed (Oxford Online Dictionary, 2017), was discussed as well as related definitions such as corporate governance, IT governance, data governance and privacy governance. The concepts of *framework* and *privacy governance framework* were also discussed. This was followed by a scoping review in which four literature articles were identified to assist in identifying important components for the CPGF. In addition, four privacy governance frameworks were discussed to identify components that could be included in the CPGF.

The CPGF was proposed, consisting of four components and sub-components respectively, namely: (a) Organisational Commitment (*Leadership Commitment*; *Information Officer*; *Privacy Office*; and *Reporting*); (b) Privacy Policies and Procedures (*Privacy Policies and Procedures*); (c) Privacy Programme Controls (*Personal Information Inventory*; *Breach Handling / Incident Management*; *Service Provider Management; Communication*; *Privacy Awareness and Training*; *Risk Assessment Tools*; and *Programme Assurance / Audit*) and (d) Ongoing assessment and Review (*Ongoing Assessment and Evaluation)*.

This chapter answered the literature review research question “What would a conceptual privacy governance framework comprise?” by proposing the CPGF.
The next chapter will discuss the research design and methodology for the empirical study. The sample selection, data collection methods, statistical methods to analyse the data, and the validity and reliability instruments will be discussed.

CHAPTER 4


Empirical study: phase 2
Chapter 1: Introduction
Chapter 4: Research methodology
Introduction
Research process
Philosophical paradigm
Research Approach
Methodological choice
Research strategy
Time horizon
Techniques and procedures
Research ethics
Chapter summary
Chapter 2: Privacy background and the Protection of Personal Information Act (POPIA)
Chapter 5: Research findings
Chapter 3: Conceptual Privacy Governance Framework
Chapter 6: Conclusion, limitations and recommendations
Literature review: phase 1

Research methodology

4.1 Introduction

The general aim of this research is to develop a CPGF and to develop a valid and reliable IPGQ to assess the perception of employees on how effective the organisation governs privacy. The background to the research and literature on privacy governance has been discussed in previous chapters. This chapter provides an overview of the research methodology for this study.

Varkevisser, Pathmathan and Brownlee (2003) are of the opinion that to solve a research problem or question, systematic collection, analysis and interpretation of data is necessary. Referring to the above definition of research, this chapter provides details of the research design to ensure that the data are collected and analysed systematically. Aspects to be discussed are the philosophical paradigm, research approach, methodological choice, research strategy time horizon as well as the techniques and procedures. The research strategy describes the survey, participant selection, data collection, expert panel review and pilot testing the questionnaire as well as the data analysis techniques applicable to this study. An overview of the research ethics will also be given to ensure that the research design is methodologically sound and morally defensive to all those involved in the study (Saunders et al., 2016).

4.2 Research process

Oates (2006:7) defines research as “the creation of new knowledge, using an appropriate process, to the satisfaction of the users of the research”. The researcher, therefore, creates new knowledge by collecting sufficient and appropriate data sources that are recorded accurately and are analysed properly and presented well (Oates, 2006).

Oates (2006) suggests aspects of research, called the 6 P’s: purpose, process, participants, product, paradigm and presentation of research as a framework to conduct the research study, as depicted in Figure 4-1.

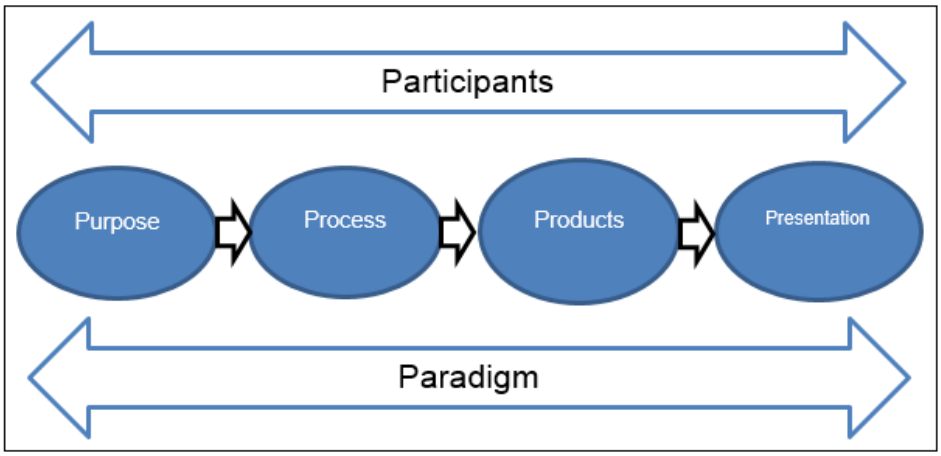


Figure 4-1: The 6 P's of research (Oates 2006:12)

- The **purpose** of the research is the reason for doing the research, the topic of interest and the importance of studying the topic (Oates, 2006). As discussed in Chapter 1 (sections 1.3 and 1.4), the research questions and objectives are defined.
- The **process** of the research is the sequence of activities during the research which includes the development of a conceptual framework, data generation methods, analysis of the data, drawing conclusions and recognising any limitations of the research study (Oates, 2006). Section 1.8 of chapter 1 discusses the sequence of activities for this research study which includes the literature review phase and the empirical study phase.
- The **products** aspect, as per Oates (2006), discusses the outcomes of the research, such as the dissertation report, conference paper, the CPGF as well as a reliable and validated IPGQ.
- **Participants** are the people who are directly involved in the research study, such as the researcher, respondents of the questionnaire (sample) and the editors of the research paper (reviewers, language editor and statistician). Oates (2006) also suggests that, during the process of the research, the researcher must deal with these people legally and ethically to avoid any physical, mental or social harm.
- **Paradigm** is a shared way of thinking, model or pattern. There is, therefore, an underlying paradigm which guides the research study. Oates (2006) discusses the following philosophical paradigms, namely positivism, interpretivism and critical research. These paradigms will be discussed in the following section of

this chapter with a motivation for the chosen paradigm of this study. For this study, the researcher has applied the positivism paradigm.

- **Presentation** is the way in which the research is explained to others; for example, a written dissertation or the presentation of a conference paper. Oates (2006) suggests that it must be carried out professionally.

Saunders et al. (2016) provide a complete research methodology in the form of a research 'onion' (Figure 4-2) that depicts the research philosophies, approaches, strategies, choices, time horizons and lastly, the techniques and procedures that will fulfil the 6 Ps of Oates's (2006) view on research. This research study will apply Saunders et al.'s (2016) research 'onion' to answer the research questions in Chapter 1 (section 1.3) and to achieve the research objectives in section 1.4.

As discussed in Chapter 1 (section 1.8), this research consists of two phases depicted in Figure 4-3, namely, the literature review phase and the empirical study phase.

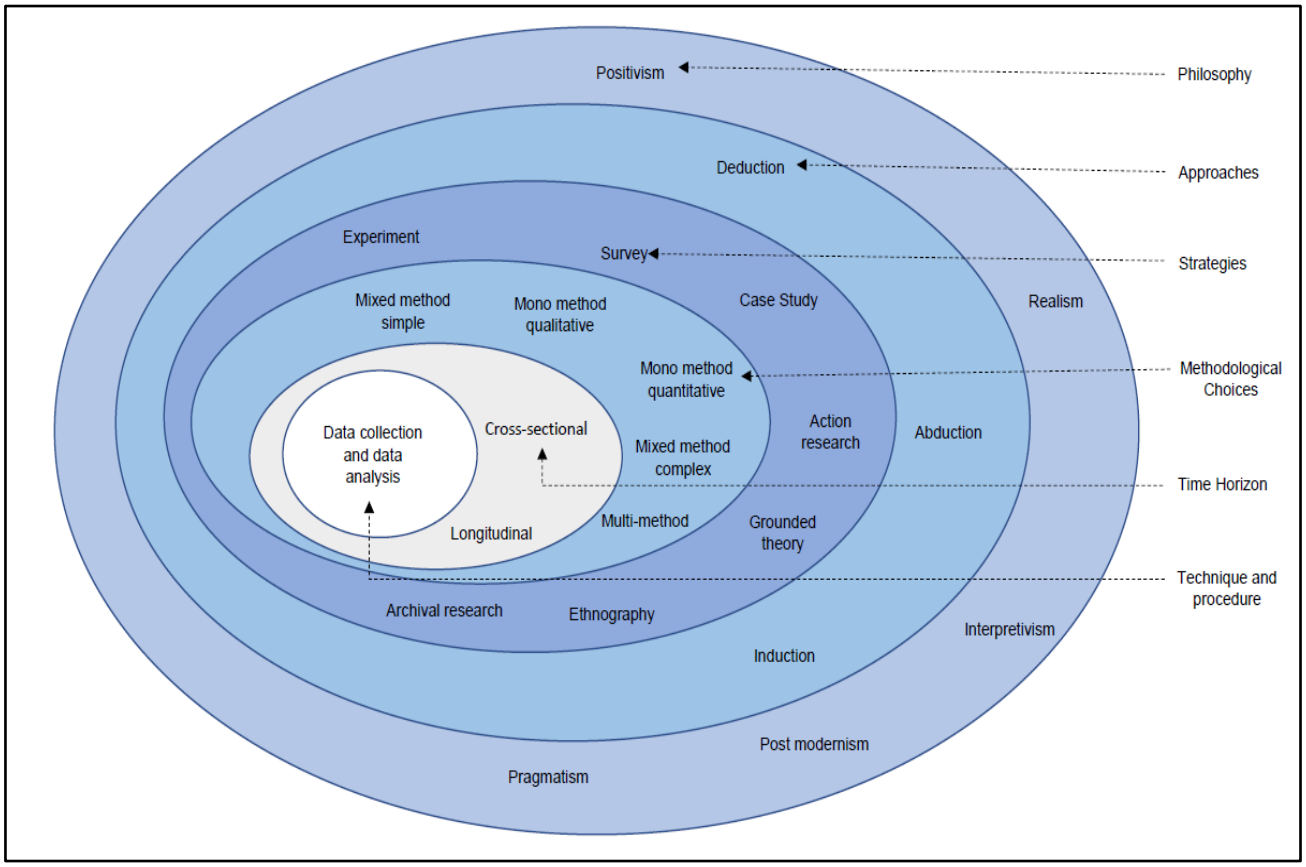


Figure 4-2: The research 'onion' (Adapted from Source: Saunders et al., 2016)

The literature review phase follows three steps namely:

- Step 1 – Background study relating to privacy and the various global privacy laws as well as the POPIA is discussed.
- Step 2 – Privacy governance is defined which is derived from various governance types such as corporate governance, data governance and IT governance to define privacy governance. A CPGF is conceptualised from various privacy governance frameworks and governance theory.
- Step 3 – The CPGF is used as the foundation for the IPGQ development.

Both phases describe the research steps as well as the output of each phase and the role players who are active during each phase.

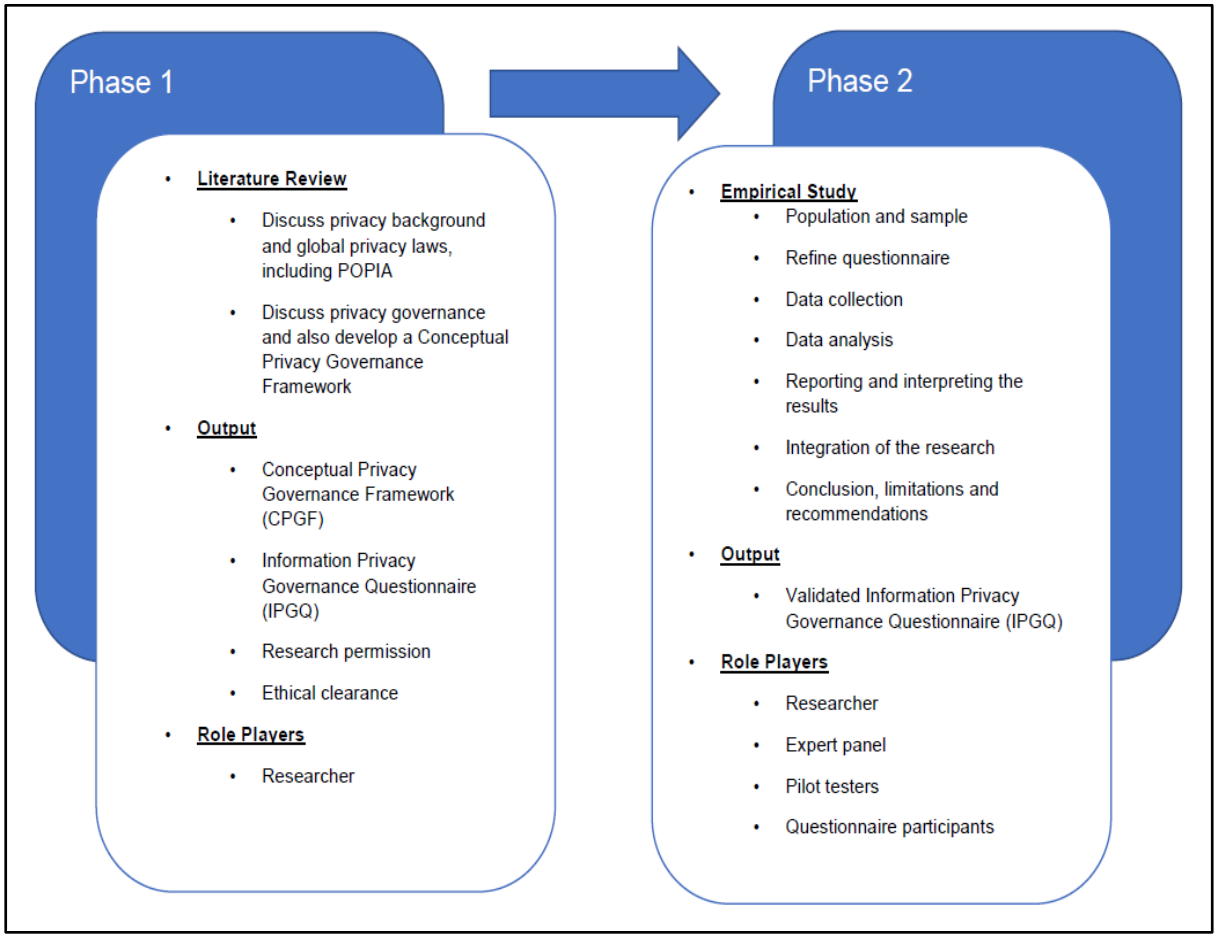


Figure 4-3: Research process (Source: Researcher)

In the next section, the philosophical paradigm of the research will be discussed as well as the subsequent layer of the research 'onion' and how it relates to the current research study.

4.3 Philosophical paradigm

In this section, the researcher will discuss the outer layers of the research 'onion' suggested by Saunders et al. (2016). This 'onion' comprises the research philosophies. Oates (2006:282) defines a paradigm as "a set of shared assumptions or ways of thinking about some aspect of the world". The different assumptions are ontology which entails the nature of reality, epistemology which is concerned with the acquiring of valid, acceptable and legitimate knowledge, and lastly, axiology which refers to the role of values and ethics during the research process (Saunders et al, 2016). Saunders et al. (2016) and Oates (2006) highlight a few common philosophy paradigms such as positivism, interpretivism for business and computing research as well as critical realism. For this study, the positivism paradigm will be discussed in the next section.

4.3.1 Positivism

Positivism is one of the oldest paradigms and is concerned with the social reality which produces law-like generalisations (Saunders et al., 2016) and underlines the scientific method (Oates, 2006). Reality can be measured implicitly and explicitly by viewing it as one-way and value-free (Sobh & Perry, 2005). During the research process, the researcher is neutral and detached from the research and data to avoid influencing the findings (Oates, 2006).

The characteristics of the positivism paradigm are as follows (Saunders et al., 2016):

- Ontology: real, external, independent and ordered. One true reality (universalism).
- Epistemology: observable and measurable facts, a scientific method and a law-like generalisation. Causal explanation and prediction as contributions.
- Axiology: value-free research. The researcher maintains an objective stance and is detached from the research.
- Methods: deductive, highly structured, measurement, quantitative method of analysis.

Referring to Figure 4-1, the paradigm guides the purpose, process, products and presentation of the research process. Empirical research derives knowledge from actual experiences and is based on observation and measured phenomena (Cahoy, 2016). The ontological assumption of the quantitative paradigm is that there is a singular reality independent from the researcher, and the nature of the reality is objective (Sukamolson, 2007).

According to the axiology assumption of the paradigm, the research is value-free because the researcher is unbiased, and the researcher's feelings and thoughts will not influence the study. According to the methodological assumption of the paradigm, the research process describes the process as deductive, accurate and reliable (Sukamolson, 2007). Statistical precision, using statistical software, ensures the validity and reliability of the data and the findings.

A questionnaire, which is a product of the research process, will be used as a measured instrument to collect data; therefore, the researcher will be independent from the participants. In view of the epistemological assumption, the researcher is independent which will provide credible data from what will be researched.

The following section will concentrate on the research approach which is the second layer of the research 'onion'.

4.4 Research approach

The research approach (refer to Figure 4-3) of the research 'onion' includes the deduction, induction and abduction approaches (Saunders et al., 2016). The research approach for this study is deduction which will be discussed in the next section.

4.4.1 Deduction

Existing theories derived from the literature or which are developed by the researcher are called a deductive approach (Oates, 2006). Deduction involves rigorous testing through a series of propositions to ensure the developed theory is valid and reliable (Saunders et al., 2016). Saunders et al. (2016) suggest a few characteristics of deduction, namely:

- It explains causal relationships between variables.
- It is a collection of quantitative data.
- Its controls allow the testing of hypotheses.
- The concepts need to be operationalised to be measured quantitatively.
- Generalisation by selecting sufficient numerical sample sizes is inherent to deduction.

There are five sequential steps that show the flow of the deductive research (Saunders et al., 2016):

i. Deducing a hypothesis from the theory
ii. Operationalising, describing how the concepts or variables are to be measured
iii. Observation through research strategies
iv. Confirmation of the theory
v. Modification of the theory, if necessary, in the light of the findings

The deductive approach refers to the phases (refer to Figure 4-4) of this research study. During phase 1 the literature review is done to collect theory regarding the background of privacy, privacy laws and various privacy governance frameworks relevant to this study in order to develop the IPGQ. In phase 2, the empirical study is done to collect observations by means of a survey and sequentially, to confirm the theory by providing a reliable and valid information privacy governance questionnaire.

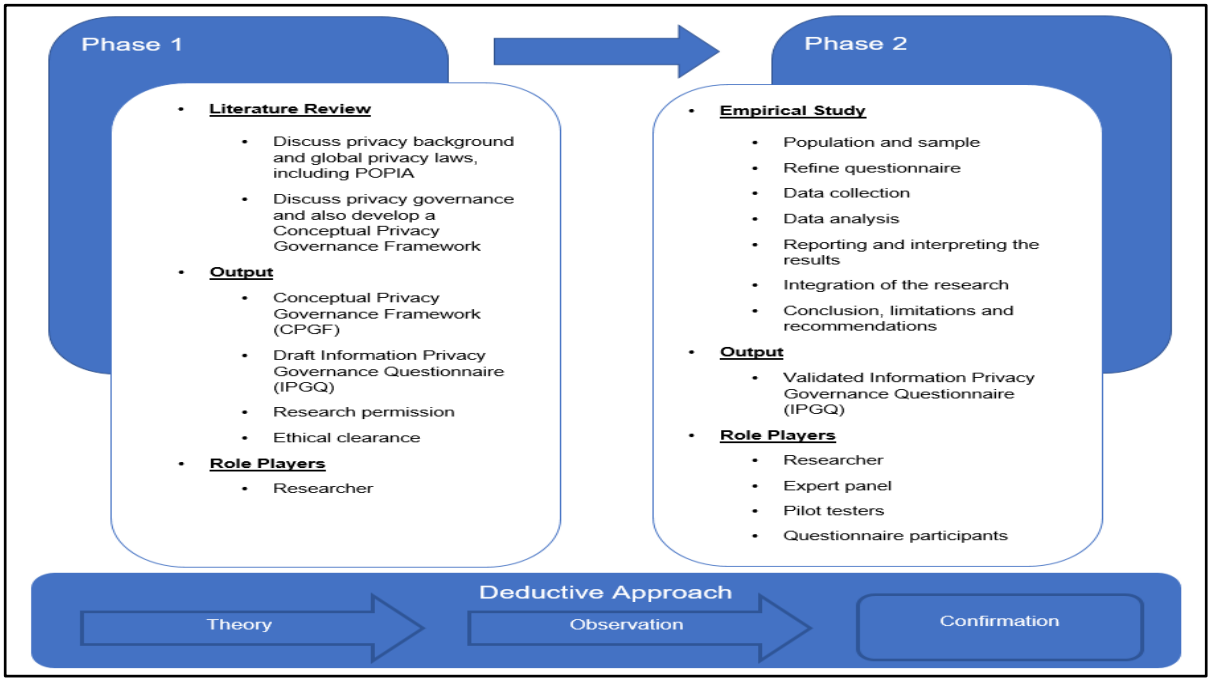


Figure 4-4: Research deductive progress (Source: Researcher)

The following section will discuss the methodological choice for this research study.

4.5 Methodological choice

The third layer of the outer layer of the research 'onion' (refer to Figure 4-5) refers to the research methodological choice.

4.5.1 Research choice

There are various research methods which will determine the research design such as the techniques to collect and analyse data (Saunders et al., 2016). When choosing the research method, a mono method (single data collection technique and analysis procedures) or multiple methods (two or more data collection techniques and data analysis procedures) can be used to answer the research questions (Saunders et al., 2016).

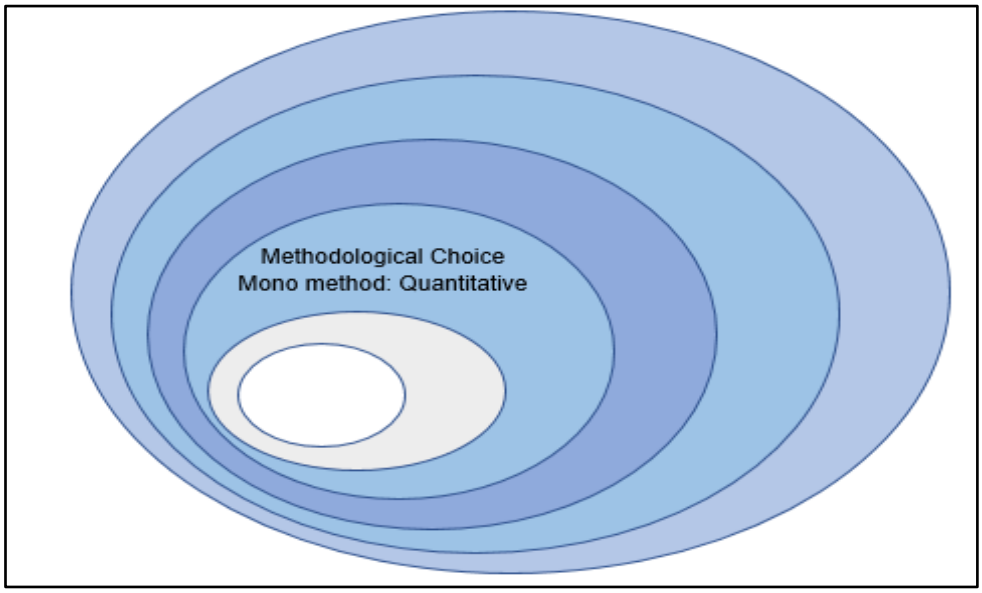


Figure 4-5: Research 'onion' – Methodological choice layer (Source: Saunders et al, 2016)

Saunders et al. (2016) mention six different types of research design, namely mono method quantitative; multi-method quantitative; mixed method simple; multi-method qualitative; mono method qualitative and mixed method complex. The mono method is a single data collection technique such as a questionnaire or interview, either in a qualitative or a quantitative study. For this study, the mono method research design was used to collect the data by means of a questionnaire which were analysed quantitatively by means of a statistical data analysis.

Figure 4-6 below illustrates the hierarchy of these research choices.

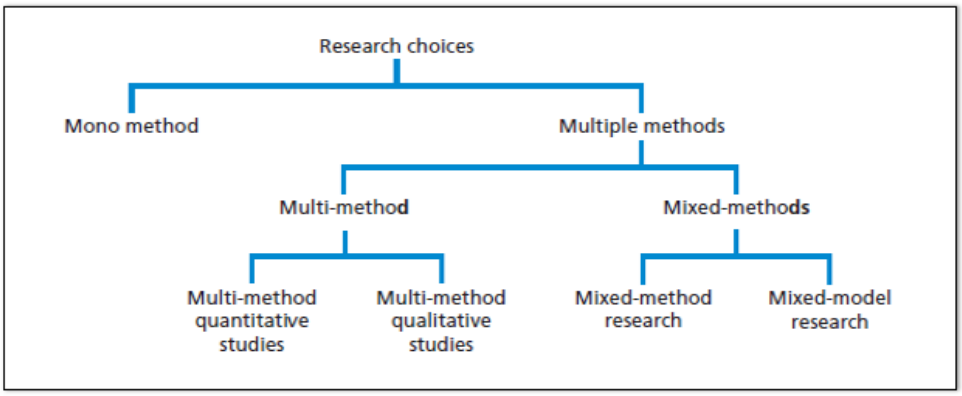


Figure 4-6: Research choices (Saunders et al., 2016)

4.5.2 Quantitative research approach

The two traditional research design approaches are quantitative and qualitative studies (Maxwell, 2012). The section below will discuss the quantitative research design approach.

4.5.2.1 Quantitative research design

Quantitative research design focuses on numeric data and is used for data collection by means of techniques such as questionnaires, or data analysis procedures such as statistics that use or generate data (Saunders et al., 2016). This approach employs empirical methods and empirical statements (Sukamolson, 2007). There are different types of quantitative research strategies, namely survey research, experimental research, correlation research and causal-comparative research (Sukamolson, 2007).

The quantitative view of this approach is realist, also known as positivist, to uncover an existing reality (Sukamolson, 2007). Objective research methods are used to uncover this reality; therefore, the researcher is separated from the research, and uses methods to make the most of objectivity and to lessen the participation of the researcher during the research (Muijs, 2004).

Advantages of a quantitative research strategy are as follows (Muijs, 2004):

- A quantitative research study is necessary when a numerical change in the study is needed.

- A quantitative answer is needed, the number of participants who fulfil the requirements of the question.
- This research strategy explains phenomena and calculates the state of something.
- It is used for testing hypotheses.

Disadvantages of quantitative research strategy are as follows (Sukamolson, 2007):

- Quantitative research is unable to explore a problem in depth.
- Variables are defined by the researcher which does not help in complex studies.
- Quantitative methods only look at cause and effect while qualitative methods will look at the meaning of a circumstance or event.

Saunders et al. (2016) suggest that quantitative research design is associated with positivism. A quantitative research entails the collection of data which are examined using scientific methods, especially statistical methods (Muijs, 2004). A quantitative research method is thus used to collect and analyse data statistically. This research method makes use of objective research methods which means that the researcher is detached from the research (Muijs, 2004). Quantitative research is also flexible because researchers can study a number of phenomena regarding the behaviours or attitudes of individuals (Sukamolson, 2007).

Sukamolson (2007:4) postulates that "(s)urvey research uses scientific sampling and questionnaire design to measure characteristics of the population with statistical precision". Questionnaires are distributed for the collection of data (Muijs, 2004). In this study, quantitative research will be conducted to develop a valid and reliable IPGQ.

4.6 Research strategy

The research strategies guide the researcher to answer the research questions and to reach the objectives of the study (Oates, 2006; Saunders et al., 2016). The choice of research strategy is guided by the research questions, philosophical belief, time, resources and existing knowledge (Saunders et al., 2016).

Oates (2012) gives an overview of the following research strategies:

- Survey – Systematically collecting similar data from a population, analysing it statistically and generalising the results to a larger population. It, therefore, provides a numeric description of trends, attitudes or opinions by studying a sample of the population (Creswell, 2014). Surveys are commonly linked with the deductive approach and primarily used in descriptive and exploratory research studies (Saunders et al., 2016).
- Design and creation – This strategy focuses on the development of artefacts, models, methods or constructs.
- Experiment – It focuses on testing hypotheses and investigating the cause and effect relationships. Experimental studies cause links between two variables (experimental and control groups) and are used primarily in exploratory and explanatory research (Saunders et al., 2016).
- Case study – It focuses on one occurrence of an object that needs to be examined such as an information system, organisation or department, decision, or discussion forum. A case study uses multiple sources of evidence to conduct an empirical investigation of a present-day phenomenon in an actual situation (Saunders et al., 2016). A case study can either be a single-case (holistic) design, multiple-case (holistic) design, single-case (embedded) design or multiple-case (embedded) design (Yin, 2009).
- Action research – This type of strategy focuses on research in action such as real-world situations and reflects on the outcome of the lessons learnt. As per Saunders et al. (2016), action research has the following strengths: (i) planning, (ii) involvement of employees (practitioners), (iii) focus on change, (iv) evaluating, (v) taking action and (vi) time devoted to diagnosing.
- Ethnography – This is a research strategy that studies a group of people in order to understand their culture. The researcher is actively involved in the life of the group of people he or she studies. The research strategy is conducted over time and the phenomenon is researched in the context in which it occurs (Saunders et al., 2016).

The research design appropriate for this research study is the non-experimental method which is popular with historical research, survey research, analysis of existing data sets and observation (Muijs, 2004). The survey research design is most popular

for a quantitative research design which is characterised by collecting data using questionnaires (Muijs, 2004). This type of research is the gathering of information in a systematic pattern from the respondents to understand and/or predict the behaviour of the population of interest (Sukamolson, 2007).

Surveys enable the researchers to collect large amounts of data from the sample population in a cost-effective way (Saunders et al., 2016). The quantitative data collected can be analysed quantitatively using inferential and descriptive statistics (Saunders et al., 2016). The data collected can therefore be used to explain possible reasons for relationships between variables and to develop models of these relationships (Saunders et al., 2016). With the sampling technique and inferential statistical analysis, the findings are representative of the whole population, and following the philosophical approach of reality, the researcher has more control over the research process (Saunders et al., 2016).

For a good survey design, Fowler Jr (2013) describes the following components that are essential to conduct a survey:

- Sampling – This is a small subset of a population, representing the wider population.
- Question design – Questions must be more objective and evaluated to improve the understanding of the question.
- Interviewing – Although not relevant to all surveys, interviewers must be trained to administer a survey, to avoid influencing the answers the respondents give and at the same time to maximise the accuracy of the answers.
- Mode of data collection – Data are collected by means of internet-based questionnaires.

Given the components for a good survey design, a sample has been taken from the wider population to represent the various business units within the organisation. The questions have been formulated to be objective and derived from the components of the CPGF developed in Chapter 3. The questions have also been evaluated by the expert panel to ensure that they conform with the legal and business requirements. The data have been collected electronically as an internet-based questionnaire.

Oates (2006) discusses five advantages of survey-based research:

i. Results are representative of the wider population, as they provide a wide and inclusive coverage of events or people.
ii. This research helps to produce a lot of data within a short period of time and at a low cost.
iii. Data can be analysed quantitatively.
iv. Surveys can be replicated, meaning that the same survey strategy can be used for a different sample or at a different time with the same group of people.
v. Surveys are suited for people with a lack of communication or interpersonal skills to conduct postal or Web-based questionnaires, documents or observations.

4.7 Time horizon

Saunders et al. (2016) discuss two types of time horizons, namely cross-sectional studies and longitudinal studies. Research studies are normally conducted over a short period of time due to time constraints or to explain an instance of a phenomenon at a given point in time (Saunders et al., 2016).

For this study, the applied time horizon is the cross-sectional study to measure the employees' perception regarding information privacy governance in the organisation, at a specific point in time. During this research period a number of departments across the organisation were included.

4.8 Techniques and procedures

In the following section, the sampling technique, data collection technique, data analysis, and data and design quality will be discussed.

4.8.1 Sampling technique

When a sample is selected from a collection or list of the whole population or events included in the survey it is called a sample frame (Oates, 2006). The sampling

technique is the method used to select people or events from the sample frame (Oates, 2006).

Saunders et al. (2016) identify two main sampling techniques:

i. Probability or representative sampling – The probability or chance for each case to be chosen carefully from the population is high and representative of the entire population.
ii. Non-probability sampling – The probability of each case to be selected from the population is unknown; therefore, the researcher is unaware that the sample or event is representative.

Referring to Table 4-1, Oates (2006) has identified four probabilistic and four non-probabilistic sampling techniques.

Table 4-1: Sampling techniques

Probabilistic	Non-probabilistic
Random	Purposive
Systematic	Snowball
Stratified	Self-selection
Cluster	Convenience

Source: Oates (2006)

4.8.1.1 Setting

The research study has been conducted in a financial institution, as it processes and stores personal information every day.

4.8.1.2 Sample

A purposive sample (a type of non-probability sample) will be used to achieve the objectives of this study (Saunders et al., 2016) because respondents from across the organisational departments have been invited to participate in the survey. The purposive sampling technique is used with small samples. The selected sample is also particularly informative (Saunders et al., 2016). The participants are selected by virtue

of their knowledge or experience, and the researcher decides on the participants who can or are willing to provide the information (Etikan et al., 2016). This sampling technique concentrates on people with particular characteristics (Etikan et al., 2016).

Respondents from different departments (Information Technology [IT], Finance, Marketing, Human Resources [HR], Operations and Privacy) were invited to complete the questionnaire. To ensure validity of the constructs, the sample size had to be approximately 5 (n) respondents to complete the questionnaire, where *n* is the total number of questions listed in the questionnaire and five is the value of the point scale (Gerber & Hall, 2017).

4.8.2 Data collection technique

Varkevisser et al. (2003) describe a data collection technique as the systematic collection of information about objects of study and the settings in which they occur. To answer the research questions, the collection of data must be systematic for the results to be conclusive (Varkevisser et al., 2003).

Oates (2006) identifies the following data collection techniques: interviews, observations, documents and questionnaires. The latter will be discussed in the next section.

4.8.2.1 Questionnaires

Questionnaires are sets of questions in a predetermined order which are mainly used in the survey strategy (Saunders et al., 2016). Saunders et al. (2016) have identified the following categories of questionnaires: self-administered and interviewer-administered. The questionnaires are self-administered and in the following section, the design and administering of the questionnaire will be discussed as well as the expert reviews and pilot testing of the questionnaire.

4.8.2.1.a Questionnaire design

The questionnaire type used for this study is the internet-mediated questionnaire which is a self-administered questionnaire. The respondents have completed the questionnaire online at a time convenient to them.

The design of the CPGF aids in the understanding of the components necessary for the IPGQ. The technique used is questionnaire-based (Pearson et al., 2009).

The focus of the IPGQ is to assess how effective privacy is governed in the organisation. It consists of a set of questions that the respondents need to answer in order to fulfil the research objectives from the information it produces (Sreejesh, Mohapatra & Anusree, 2014).

The layout of the questionnaire consists of three sections. A cover letter is included in the questionnaire to introduce the study to the respondent and to assure the respondent that the survey is anonymous and completely voluntary (Appendix C). The purpose of the survey and the participant's confidentiality are discussed in a brief introduction in the questionnaire (Sreejesh et al., 2014).

Section 1 of the questionnaire consists of six demographic questions to establish the respondent's *age, gender, employment status, job level, length of service, and business unit*. Section 2 comprise general awareness questions to determine the respondent's knowledge about information privacy policies and procedures within the organisation. A "Yes/No" scale was used for these questions. Section 3 of the questionnaire consists of 60 questions that are based on the theoretical statements of the CPGF after the expert panel review and the pilot testing has been done. A five-point Likert scale is used to obtain data regarding the respondent's privacy perception within the organisation in section 3 (refer to Appendix E).

4.8.2.1.b Expert reviews

Questionnaires must include standardised questions which must be interpreted by all respondents in the same way (Saunders et al., 2016). To ensure that the questions are relevant and interpreted by all respondents in the same way, a panel of experts reviewed the relevance, clarity and suitability of the questions in the IPGC. The questions were evaluated by experts in the information privacy domain to provide suggestions on the structure of the questionnaire (Saunders et al., 2016) before the pilot testing took place (Oates, 2006). Four columns were added to the questionnaire for the expert panel review, namely "Not essential", "Essential", "Item is clear" and "Item is unclear". Each statement was evaluated by the expert panel to indicate if the

statement was essential and clear to ensure that the respondents would understand and interpret the statements in the same way.

The criteria for selecting the experts were:

- POPIA experience and knowledge
- More than three years' experience
- Higher education
- Across domains – one expert from legal for regulatory experience, one expert from academia, one expert from compliance and one expert from privacy consulting with experience across different industries.

The expert panel consisted of four subject experts in the field of privacy and were the participants (see Figure 4-2) in the research process to evaluate the questionnaire. The experts were from different backgrounds, namely legal, academic, privacy consultancy and compliance in a financial institution to meet the fourth criteria. The expert panel had to complete section 1 – *Expert panel information sheet* – of the questionnaire (see Appendix E) which required them to capture their years of experience, highest qualification, current job title and the years of experience relating to the POPIA and privacy governance, as depicted in Table 4-2 below.

Table 4-2: Expert panel background information

Expert Panel Background Information				
	Expert 1	**Expert 2**	**Expert 3**	**Expert 4**
Field of expertise	Legal	Academic	Privacy	Compliance (Regulator)
Job title	General Counsel: Advisory Technology	Senior Lecturer	Senior consultant / architect	Compliance Officer
Information privacy experience (years)	7	5	10+	3
POPIA experience	Experience in dealing with the POPIA Bill and the Act since 2012	The POPIA was part of research studies	Six years' the POPIA experience	Implementation of compliance risk management plan for the POPIA – three years
Highest qualification	LLM (master's degree in law)	MSc (Computer Science)	Electronic Eng. Diploma	LLB, Postgraduate Diploma

For expert evaluation in the field of Human-Computer Interaction, three to five experts can be used to identify errors during heuristic evaluation (Nielsen & Landauer, 1993). The diagram (Figure 4-7) below shows the percentage of errors that can be detected by experts during their evaluation. Nielsen and Landauer (1993) state that five experts can identify 85% of the errors. From six to fifteen experts on the diagram show that it is not viable, as the experts will deliver the same result when identifying errors (Ouma, 2013). As such, four experts were used in this study, as they had extensive experience in the privacy domain as well as in the application of the POPIA.

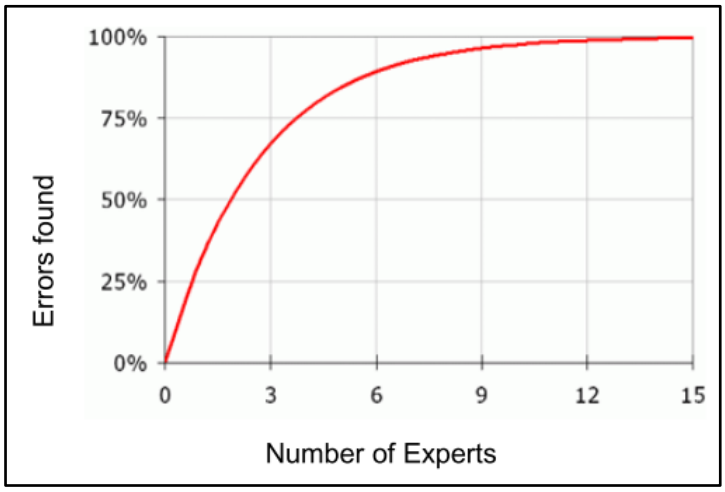


Figure 4-7: Error detection rates (Ouma, 2013)

The expert panel reviewed sections 2 and 3 of the questionnaire (see Appendix E). The feedback from the expert panel indicated that all the items in section 2 were *essential* and each *item was clear*.

The 66 (item seven to 72) items in section 3 were reviewed by the expert panel who indicated that 37 items of the 66 were not essential and that 17 of the 66 were unclear (54 in total). Table 4-3 lists all the items that have been identified by the expert panel as not essential and/or unclear. The table only shows the results of three experts, because the fourth expert has indicated that all the items in section 2 and section 3 are essential and clear.

The items in table 4-3, which are highlighted in red, are common items that have been identified by all three of the expert panel members. There are 10 items for the 37 items that have been indicated as *not essential*, namely 8, 11, 12, 14, 24, 42, 49, 60, 61 and 62. These 10 items were removed. There are two items that are common for the 17 items identified as *unclear*, namely 51 and 57 and have been revised. Three items that have been highlighted as both *not essential* and as *unclear*, namely 66, 67 and 68, have been removed from the questionnaire. Item 49 has been moved to section 2 as a general awareness question. Thirty nine of the 54 items identified by the three experts as either *not essential* and *item not clear* have been retained and revised for a better understanding so as to also comply with the market and privacy regulatory requirements.

Table 4-3: Expert panel – "Not essential" and "Item is unclear"

Not Essential				**Item is unclear**			
Expert 1	**Expert 2**	**Expert 3**	**Expert 4**	**Expert 1**	**Expert 2**	**Expert 3**	**Expert 4**
8**	8**	25		11	63	9	
11**	10	32		12	67**	29	
12**	11**	52		14		35	
14**	12**	62**		22		51	
15	14**	61**		37		57	
16	19			39			
17	23			46			
18	24**			51			
22	25			52			
24**	37			57			
30	42**			66**			
42**	43			67**			
46	44			68**			
49*	45						
57	49*						
58	55						
59	61**						
60**	67**						
61**							
62**							
63							
64							
65							
67**							
68**							
70							
*** Moved to section 2** **** Removed from questionnaire**							

The expert review panel's general comments were aimed at the understandability of the questions, and they asked for the questions to be rephrased for a clearer understandability. The expert panel commented that the employees' general knowledge of privacy aspects should be considered in order for them to answer the questions in section 3. They also highlighted that some of the questions might not be applicable to all departments or different employee job levels; therefore, they requested for the questions to be generalised.

4.8.2.1.c Pilot testing

Oates (2006) suggests that the questionnaire needs to be piloted first by a group of people who will complete the questionnaire as if they are the target population.

The purpose of the pilot testing is to refine the questionnaire so that the target respondents will have no problems answering the questions, and the collected data will be reliable and valid (Saunders et al., 2016). The improvements suggested by the pilot group help with the design of the questionnaire (Cooper & Schindler, 2014). The pilot testing also helps with the face validity of the questions to test whether the questionnaire appears to make sense (Creswell, 2014; Saunders et al., 2016).

Oates (2006:226) identifies five aspects regarding the trial run of the questionnaire that will assist the researcher in identifying the shortcomings of the questionnaire:

i. "People experience difficulties answering certain questions.
ii. Ambiguous or vague questions are identified.
iii. Is the instruction clear to follow?
iv. Do pre-defined responses cover all desired answers?
v. Duration time to complete the questionnaire: Is it a reasonable time?"

The process followed for the pilot-testing group was as follows:
A group of 10 people from different departments in the selected financial organisation was selected for the pilot-testing group. Each of the participants of the pilot group received a consent form (see Appendix D) to participate in the study as well as a participant information sheet that described the research study (see Appendix C). It took the participants on average 15 minutes to complete the IPGQ (Appendix F). Participants were asked to pay attention to the questions regarding the grammar and if the questions were understandable and clear. After all the participants had

completed the questionnaire, a short discussion was held to revise the content of the questions as well as the five aspects described by Oates (2006) in the previous paragraph. The discussion session was facilitated by the co-supervisor.

The general perception of the pilot group was very positive, and all the participants were comfortable answering the questions. The participants were comfortable with all the questions and they did not recommend any changes to the biographical and general awareness questions. As the presentation for the last step in the research process suggested by Oates (2006), open-ended questions were suggested by the pilot group. These were included at the end of the final questionnaire for the participants of the survey to add their comments.

4.8.2.1.d Final IPGQ

The final IPGQ (see Appendix G) consists of the instructions page, section 1: Biographical Information, section 2: General Awareness, section 3: Privacy Governance Perception, and lastly, one open-ended question. Each of the sections are discussed below. The IPGQ was called “Privacy Perception Questionnaire” for the survey in the organisation.

Instructions

The participants are thanked for their willingness to participate and the background of the study is provided. Instructions and definitions are provided to guide the participants in completing the questionnaire as well as to understand the terminology in the questionnaire. Participants are informed regarding the duration for completing the questionnaire and that the survey can be completed in one session.

Section 1: Biographical Information

The biographical information section consists of six statements. Instructions on how to complete the section is provided before the participant answers the questions. The participants must select their answer from a list of pre-populated options. The following biographical information was requested from the participants:

- Age
- Gender
- Employment status

- Job level
- Length of service
- Business unit

Section 2: General Awareness

This section consists of eight statements for the participants to answer. Instructions are given to complete the section. This section tests the participants' general awareness of privacy and a "Yes/No" scale is used for the participants to select their options.

Section 3: Privacy Governance Perception

This section consists of 60 statements and one open-ended question for participants to note their comments. The section is subdivided, whereby statements are grouped into subsections that are linked to the components of the CPGF. The subsections are as follows: *Leadership Commitment*; *Information Officer*; *Privacy Office*; *Reporting*; *Privacy Policies and Procedures*; *Personal Information Inventory*; *Breach Handling / Incident Management*; *Service Provider Management; Communication*; *Privacy Awareness and Training*; *Risk Assessment Tools*; *Programme Assurance / Audit*; and *Ongoing Assessments and Evaluation.*

The Likert scale is used for the respondents to select their answer for each statement. Responses for each statement are marked according to a five-point scale:

- Strongly disagree = 1
- Disagree = 2
- Neutral = 3
- Agree = 4
- Strongly agree = 5

4.8.2.1.e Administering the questionnaire

Hard copies of the questionnaire were distributed to the expert panel and pilot group, and an electronic questionnaire was distributed to the employees of the organisation. The end-users of the financial institution, respondents from the various departments within the organisation, completed the final IPGQ. The survey was distributed electronically so that the end-users were able to access the survey by means of a

hyperlink to the survey site. An online survey organisation was used to design and host the questionnaire online which was accessible from the financial institution. SurveyTracker software was used by the company to administer the questionnaire responses and to update the researcher on the progress of the responses received.

4.8.3 Data analysis

Data analysis is part of the process for analysing the collected data during the survey. In the following section, descriptive and inferential statistics (factor and item analysis), which are products of the statistical outcome, will be discussed. The data will also be presented in graphical and tabular formats for interpretation.

4.8.3.1 Descriptive statistics

Descriptive statistics allow the researcher to describe and compare the variables numerically (Saunders et al., 2016). Two aspects, namely the central tendency and the dispersion, describe a variable statistically (Cooper & Schindler, 2014).

General impressions of values that could be seen as average, common or middling are termed ‘measures of central tendency’ (Saunders et al., 2016). There are three ways of measuring the central tendency, namely the mode (frequent occurrence of a value), median (middle value after data have been ranked) and the mean (also known as the average of data values) (Cooper & Schindler, 2014). Dispersion is data values that are dispersed around the central tendency values.

In this study, the distribution of the data is displayed in graphical formats to depict the spread and shape of the distribution of the sample and the population.

4.8.3.2 ANOVA

Analysis of Variance (ANOVA) is a statistical method used to test the null hypothesis that the means of several populations are equal (Cooper & Schindler, 2014). The One-way ANOVA was used in this study. It is a simple ANOVA that uses a single factor to compare the effects of another factor (Cooper & Schindler, 2014). Scheffé’s multiple comparison test was used to compare the mean differences at a significance of a 0.05 level (Chu & Liao, 2010; Cooper & Schindler, 2014). The aim of the One-way ANOVA

was to determine if the perception of how effective privacy was governed in the organisation differ according to age, gender, employment status, job level, length of service and business unit groups of the respondents.

The following one-way ANOVA was employed in this research study:

- One-way ANOVA between age groups.
- One-way ANOVA between employment statuses.
- One-way ANOVA between job levels.
- One-way ANOVA between business units.
- One-way ANOVA between lengths of service.
- One-way ANOVA between gender groups.

4.8.3.3 Validity

Saunders et al. (2016:157) describe validity as whether the research findings "are really about what they appear to be about". When evaluating tests, validity is a crucial consideration, and no findings can be published without validation studies having been conducted (McCowan & McCowan, 1999). There are different types of validity, namely face validity, content validity and construct validity (McCowan & McCowan, 1999).

4.8.3.3.a Face validity

Face validity is defined as an "agreement that a question, scale, or measure appears logically to reflect accurately what it was intended to measure" (Saunders et al., 2016:592). An expert panel and pilot group reviewed the statements in the questionnaire. The expert panel and pilot group had to verify whether each statement was clear and understandable before the final questionnaire could be administered.

4.8.3.3.b Content validity

Content validity measures the adequacy of the investigative questioning coverage guiding the study (Cooper & Schindler, 2014). For the research phase of the literature review, content validity was used when evaluating the components and sub-components to be included in the CPGF from other privacy governance frameworks discussed in Chapter 3. The theoretical concepts were used to derive statements that were included in the questionnaire. An expert panel helped with the content validity of the questionnaire in order to evaluate whether the questions were *essential*, *not essential*, *clear* or *unclear*.

4.8.3.3.c Construct validity

The latter type, construct validity, is the initial question, concept or notion that determines how data are to be gathered (Golafshani, 2003). Factor analysis is used with construct validity (Cooper & Schindler, 2014), and the factor loadings, also called coefficients, indicate how closely the variables are related to each factor (Sreejesh et al., 2014).

Factor analysis aims to simplify complex sets of data by means of statistical techniques (Kline, 1994). EFA is one of the main factor analysis techniques (Gie Yong & Pearce, 2013). EFA explore datasets and tests predictions to uncover complex patterns (Gie Yong & Pearce, 2013). Factor analysis groups common variables into descriptive categories by reducing large datasets that consist of several variables in observable groups of variables (i.e., factors) (Gie Yong & Pearce, 2013). In this study, EFA has been used, as it is a newly developed questionnaire. Principal axis factoring is used to extract the factors with Oblimin rotation to obtain a new set of factor loadings.

4.8.3.4 Reliability

Reliability is also termed ‘consistency’ (Saunders et al., 2016). It measures the consistency of a questionnaire to ensure that it will produce consistent findings under different conditions and at different times (Saunders et al., 2016). Three different approaches to assess reliability will be considered at the design stage of the questionnaire, namely test re-test, internal consistency and alternative form. Internal consistency measures the consistency of responses with the questions or a subgroup of the questions in the questionnaire (Saunders et al., 2016). Since Cronbach’s alpha coefficient is the most frequently used method to calculate internal consistency (Saunders et al., 2016), it is used in the proposed study to measure the reliability of the statistical dimensions or factors. A score above 0.70 is a desirable score to establish reliability (Esterhuizen & Martins, 2016).

4.9 Research ethics

Three broad sets of considerations, namely practical, technical and ethical considerations, shape surveys (De Vaus, 2013). According to the author, ethical considerations shape the final design of the respective survey, such as ethical issues

that arise during the collection of survey data and the responsibilities towards the survey respondents and those to the colleagues.

During this quantitative research, there are various people who will be affected by this research, namely the research participants and professional colleagues. This research adheres to the UNISA policy on research ethics to conduct the research responsibly and to protect the rights of the research participants. All participants in the research are informed that the survey is voluntary, confidential, their anonymity will be guaranteed and their privacy will be protected, with no harm to them. These are the ethical responsibilities the researcher has towards the research participants (De Vaus, 2013).

A “Consent to participate” form applicable to the research objective was drafted and completed by all the research participants to have their consent on file. This is another one of the ethical responsibilities postulated by De Vaus (2013). Before the survey was conducted, an application for ethical clearance was submitted to the Ethical Committee within the School of Computing where after the approved research ethics certificate was issued (Appendix B). Permission to conduct the survey was acquired from the departmental heads of the organisation (Appendix A) and the respondents completed the consent form (Appendix D) to participate in the study.

4.10 Chapter summary

The aim of this chapter was to describe the research methodology that guided the research process to answer the research questions. Figure 4-2 illustrates the research methodology used that guided this research based on the research ‘onion’ developed by Saunders et al. (2016).

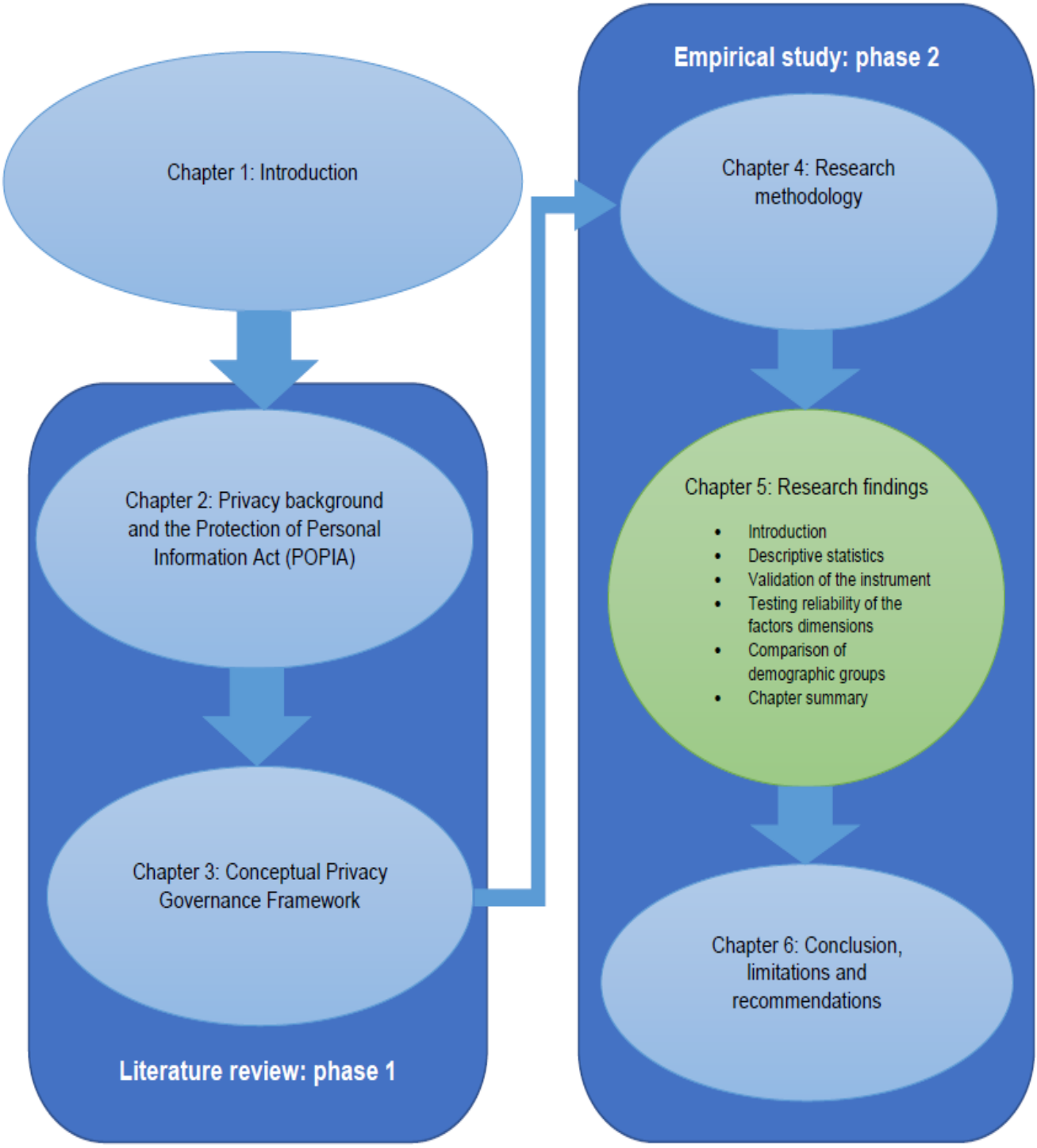
As discussed in this chapter, the research philosophical paradigm chosen for this study is the positivism paradigm, as it allows the researcher to be objective of the reality, while the empirical research is based on observation and measured phenomena. The research approach chosen for this study is the deductive approach. For the collection and analysis of the data, the mono method quantitative methodological method has been chosen.

The research strategy discussed in this chapter is the survey which is selected to collect the same kind of data from a group of people. The cross-sectional time horizon has been discussed, as business processes change over time. Lastly, the technique and the procedure for conducting this study are questionnaires to collect the data. Statistical methods have been used to analyse and interpreted the data in line with the required ethics requirements.

The questionnaire was sent to an expert panel to verify if each statement was clear and essential. After reviewing the feedback from the expert panel, the questionnaire was updated and then sent to a pilot group to verify if each statement in the questionnaire was clear and understandable. The final questionnaire was then developed and administered online at the financial institution to collect the data in line with the required ethics requirements.

In the following chapter, the results of this study will be discussed and analysed.

CHAPTER 5


Chapter 1: Introduction
Chapter 2: Privacy background and the Protection of Personal Information Act (POPIA)
Chapter 3: Conceptual Privacy Governance Framework
Literature review: phase 1
Empirical study: phase 2
Chapter 4: Research methodology
Chapter 5: Research findings
Introduction
Descriptive statistics
Validation of the instrument
Testing reliability of the factors dimensions
Comparison of demographic groups
Chapter summary
Chapter 6: Conclusion, limitations and recommendations

Research findings

5.1 Introduction

The general aim of this research study is to develop a CPGF that can be used to develop a valid and reliable IPGQ to assess the perception of employees on how effective the organisation governs privacy. This aim addresses empirical research questions 1 and 2.

The objective of the empirical research questions, as referred to in section 1.3.2 of Chapter 1, is to validate and test the reliability of the measuring instrument, and to determine the employees' perceptions on how effective the organisation governs privacy.

The following results will be discussed in this chapter:

- Demographical profile of the sample and the number of responses in the survey
- Responses received for the privacy background statements
- EFA results to determine the factorial structure as the validation of the instrument
- Cronbach Alpha test results to establish the internal reliability of the factors
- ANOVA test results to establish the significant differences among the demographic groups

5.2 Descriptive statistics

In the following sections, the demographic profile of the sample and the privacy background statements will be discussed.

5.2.1 Demographic profile of the sample

A total of 377 respondents participated in the online survey conducted at a financial institution in South Africa. The financial institution has branches countrywide, and for this study a specific location was selected, namely Johannesburg. According to Krejcie and Morgan (1970), a sample size of 380 is adequate for a total population of 31 401, with a confidence level of 95%. In Table 5-1, a brief summary of the organisation's

employment profile is given with female employees at 60% and male employees at 40% of the total employees. The total number of contractors/vendors (temporary employees) is 5% of the total number of employees in the organisation.

Table 5-1: Organisation employment profile

Total Employees in South Africa			**Total Population**			
	Male		**Female**		**Total**	
Permanent	37%	11 618	58%	18 213	95%	29 831
Contractors/Vendors	3%	942	2%	628	5%	1 570
Total	40%	12 560	60%	18 841	31 401	

The demographic statements consisted of the first six questions of the questionnaire. In this section, the age distribution, employment status, job level, gender, length of service and business unit will be discussed.

5.2.1.1 Age distribution

As illustrated in Figure 5-1 below, the age distribution of the sample varies across four categories from 18 to 72 years. The largest group of respondents was born between 1981 and 2000. Of the sample, most participants were between 18 and 37 years of age (59.2%). The lowest percentage of participants (1.9%) fell into the 64 to 72 age.

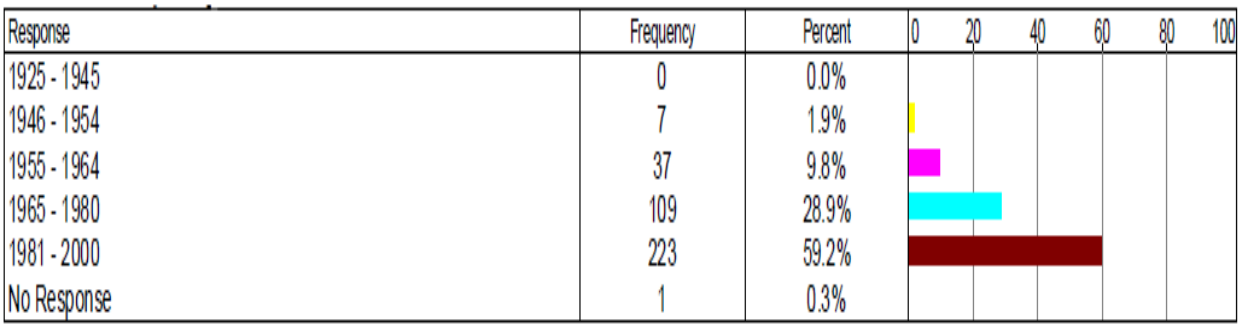


Figure 5-1: Age group distribution (n = 377)

Figure 5-2 displays the age distribution for the population. For an age distribution requirement, the sample is representative of the population with most employees who are between the ages of 18 to 37.

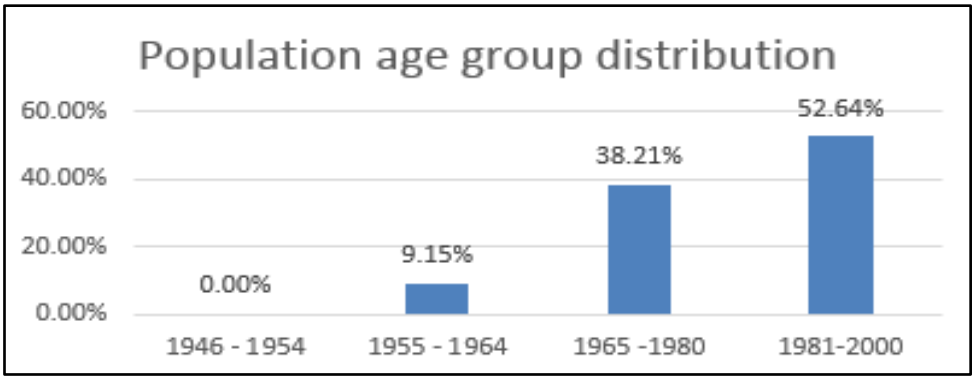


Figure 5-2: Population age group distribution (n = 29870)

5.2.1.2 Gender distribution

The sample consisted of 55.4% males and 44.3% females as illustrated in Figure 5-3 below.

Response	Frequency	Percent
Male	209	55.4%
Female	167	44.3%
Prefer not to disclose	1	0.3%
No Response	0	0.0%

Figure 5-3: Gender distribution (n = 377)

One person preferred not to disclose his/her gender. Referring to Table 5-1 above, the gender distribution for the population was 40% male and 60% female. More female participants participated in the survey than the population distribution of the male employees. This could be related to the number of females employed in the particular business units that participated. Figure 5-4 displays the gender distribution for the population. The difference between the sample and population figures is not large though.

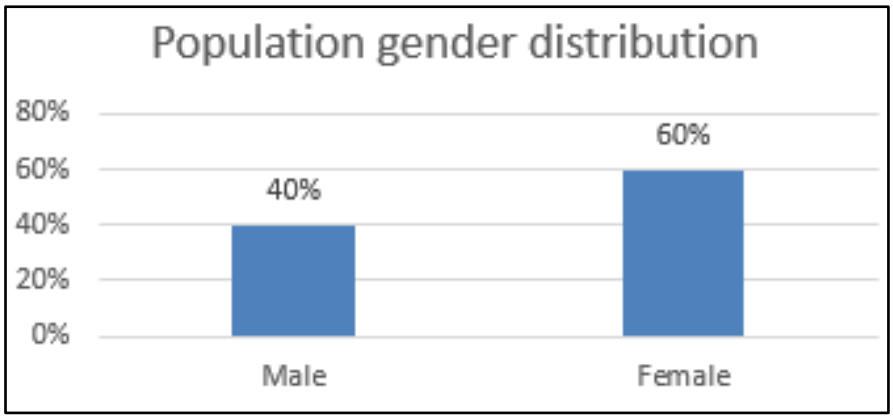


Figure 5-4: Population gender distribution (n = 31 401)

5.2.1.3 Job level distribution

Most of the respondents were employed at operational level, representing 53.1% of the research sample, as illustrated in Figure 5-5. Team leaders and line managers show a similar distribution of 9.3% and 8.5% respectively.

Response	Frequency	Percent
Administration	95	25.2%
Operational	200	53.1%
Team Leader	35	9.3%
Line Manager	32	8.5%
Senior Management	10	2.7%
Executive	2	0.5%
No Response	3	0.8%

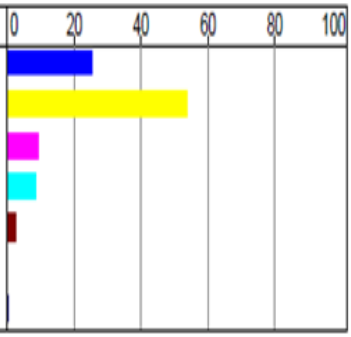


Figure 5-5: Job level distribution (n = 377)

Figure 5-6 displays the job level distribution for the population. The representation of the sample for Operational (53.1%) and Administration (25.2%) is well-represented compared to the population distribution where operational staff represents the job level with the most employees in the organisation. For the job level group overall, the sample is well-representative of the population.

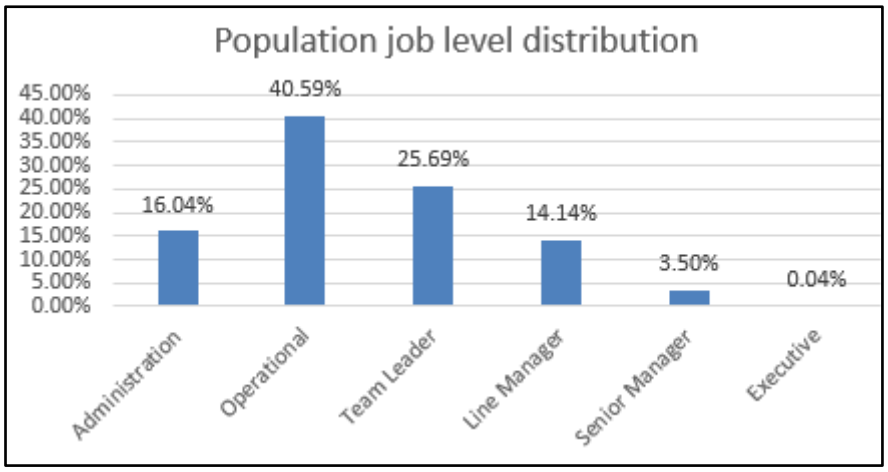


Figure 5-6: Population job level distribution (n = 29 870)

5.2.1.4 Employment status distribution

For this research sample, most of the respondents were permanent employees of the organisation with a percentage of 71.9% while the contractors and vendors with a combined percentage of 27.8%, as illustrated in Figure 5-7 below.

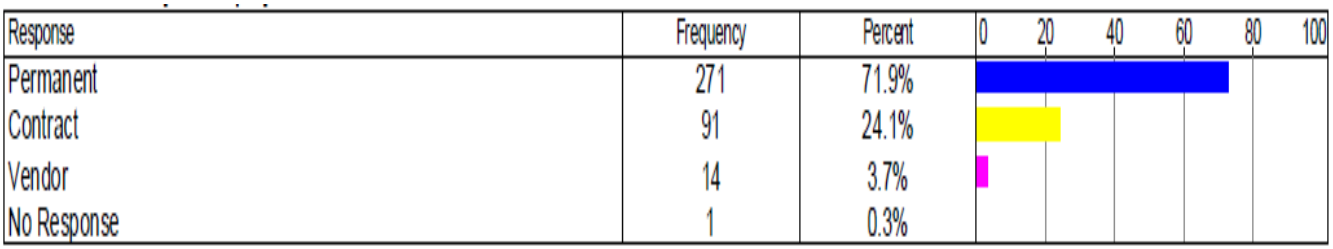


Figure 5-7: Employment status distribution (n = 377)

The population distribution, as illustrated in Table 5-1, shows that the permanent employees make up 95% of the employees and the contractors/vendors (temporary employees) make up 5%. The contractors and vendors combined in the sample (27.8%) are thus somewhat over-represented compared to the population (4.88%), as illustrated in Figure 5-8.

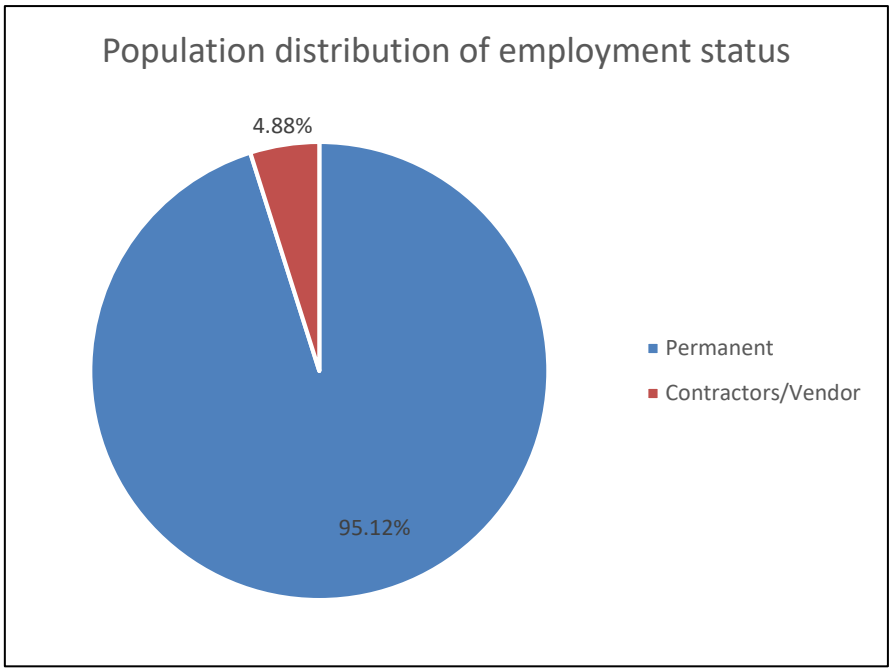


Figure 5-8: Population distribution of employment status (n = 31 401)

5.2.1.5 Length of service

The distribution of the employee's length of services is almost distributed equally for employees with 1-3 years and 10 years and more for the organisation in the study with a percentage of 33.7% and 34% respectively, as illustrated in Figure 5-9. Length of service groups 4-6 years and 7-9 years are 24.9% and 6.9% respectively.

Response	Frequency	Percent	0 20 40 60 80 100
1 - 3 years	127	33.7%	
4 - 6 years	94	24.9%	
7 - 9 years	26	6.9%	
10 years and more	128	34.0%	
No Response	2	0.5%	

Figure 5-9: Length of service (n = 377)

Figure 5-10 displays the overall distribution of the sample as well-represented compared to the distribution of the population where the organisation's workforce is mostly represented by staff employed for 10 years or more, followed by those with 1-3 years of service.

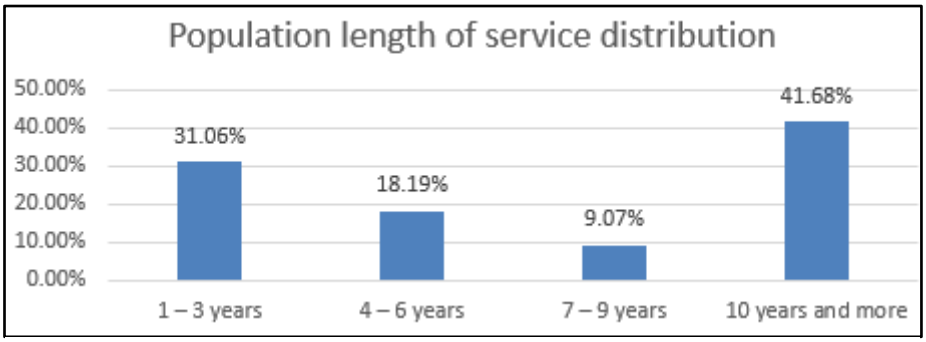


Figure 5-10: Population length of service (n = 29 870)

5.2.1.6 Business unit distribution

As illustrated in Figure 5-11 below, the largest distribution of the business unit category is IT with a percentage of 56% and the second largest is Retail or Business Banking with a percentage of 17.5%. The questionnaires were distributed at the IT department campus and some of the individuals were not affiliated with the IT department, but with other business units. These respondents who are not affiliated with the IT department work closely with the business unit to enhance the IT systems. The comparison between the sample and the population in terms of the business unit groups is not available.

Response	Frequency	Percent
Finance	19	5.0%
HR	6	1.6%
Insurance	17	4.5%
Investment Banking	3	0.8%
IT	211	56.0%
Legal	0	0.0%
Marketing or Communication	2	0.5%
Operations	29	7.7%
Retail or Business Banking	66	17.5%
Risk or Compliance or Auditing	0	0.0%
Other	24	6.4%
No Response	0	0.0%

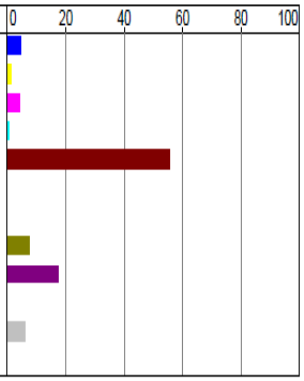


Figure 5-11: Business unit distribution (n = 377)

5.2.2 Results for the privacy knowledge questions

Eight knowledge questions were asked during the survey in section 2 of the IPGQ, using a scale of “Yes” or “No”. The results are presented in Figure 5-12. Most of the participants (93.1%) answered “yes” for completing the mandatory privacy compliance test which is an indication that the participants were aware of the privacy compliance requirements, policies and privacy controls that were in place. A further 87.5% of the

employees read the Data Privacy Policy and 77.7% knew where to get a copy of the policy. The results showed that 81.4% were aware that there was a privacy notice on the financial institution website. Also, 74.3% of the participants received privacy training when they joined the organisation and 60.5% received privacy training in the last year. The results showed that 56% of the employees knew who the Information Officer was and 43% were unaware who the Information Officer was.

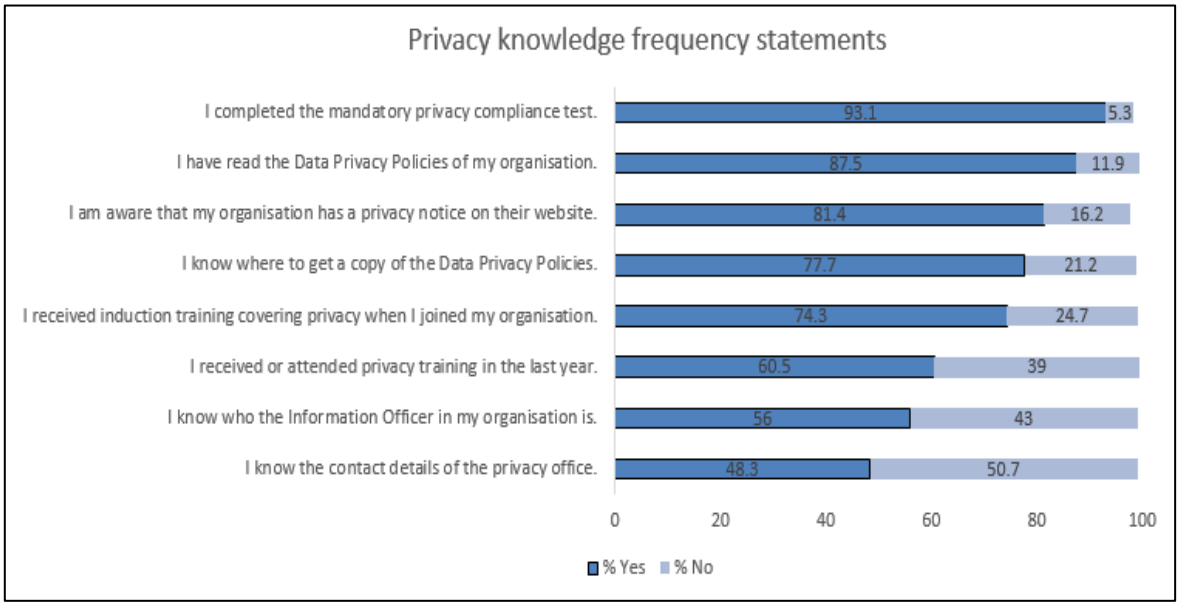


Figure 5-12: Privacy knowledge frequency statements (Source: Calculated from statistical data)

The results showed that half of the participants (50.7%) were not aware of the privacy office contact details; therefore, the communication regarding the contact details was not clear.

5.2.3 Results for the privacy governance perception questions

For section 3 of the IPGQ, 60 questions were asked during the survey, using the Likert scale (strongly disagree, disagree, neutral, agree and strongly agree). For this section, statements with the highest mean value and statements with the lowest mean value will be discussed.

Table 5-2 shows the top ten and bottom ten statements mean values. The mean values are sorted from the highest to the lowest for each statement.

Table 5-2: Mean value of top and bottom ten statements

Top ten statements – Mean value	
Statements	**Mean**
Q15_S1: 15. My organisation is committed to the protection of personal information.	4.48
Q39_S1: 39. I know how to identify personal information.	4.36
Q40_S1: 40. I know how to identify special (sensitive) personal information.	4.35
Q49_S1: 49. I am aware of the harmful effects (e.g. my organisation's brand and reputational damage, loss of market share and revenue, customer distrust or legal action against the company) of the violation of privacy policies and procedures.	4.33
Q17_S1: 17. I believe that my organisation effectively governs the protection of personal information with which we work.	4.31
Q46_S1: 46. I am aware of the consequences of the violation of privacy policies and procedures.	4.3
Q62_S1: 62. My organisation expects me to complete an annual privacy compliance test.	4.29
Q63_S1: 63. The privacy training helps me to understand how to protect personal information.	4.29
Q24_S1: 24. My organisation ensures that personal information is protected in all our applications.	4.28
Q26_S1: 26. I have received clear communication from my organisation regarding privacy requirements (e.g. how to protect customer data).	4.27
Bottom ten statements – Mean Value	
Statements	**Mean**
Q16_S1: 16. Management provides me with adequate guidance to implement the regulatory requirements of the Protection of Personal Information Act (POPIA) of 2013 in my daily duties.	4.06
Q48_S1: 48. I am aware of the timeframe to report a personal data compromise (privacy breach).	4.06
Q54_S1: 54. My organisation informs me about my privacy rights.	4.06
Q31_S1: 31. I am aware of the timeframe to report a personal data compromise (privacy breach).	4.01
Q74_S1: 74. My business unit regularly receives privacy practice updates.	4.01
Q27_S1: 27. I am aware of the role of the Privacy Office.	4
Q30_S1: 30. The reporting structures for privacy are clear in my organisation.	3.99
Q56_S1: 56. My organisation will notify me if my personal information has been compromised.	3.99
Q60_S1: 60. Privacy training is customised for my job role.	3.9
Q20_S1: 20. We are encouraged to obtain input from the Information Officer for important business decisions.	3.76

Figure 5-13 below shows the frequencies for the statements with the highest mean values. The graph shows the frequencies for each statement according to the Likert scale values for the data collected. With an average of 48%, the *strongly agree* scale is the highest, followed by the *agree* scale with an average of 40%. For the top ten statements, the average for *neutral* is 11%, for the *disagree* scale it is 2% and lastly, for the *strongly disagree* scale it is 0%.

The responses for the top ten statements for the *agree* and *strongly agree* scales are almost evenly spread, and represent the following dimensions: *Leadership Commitment, Personal Information Inventory, Breach Handling / Incident Management, Privacy Awareness and Training, and Privacy Office*. For the top three statements, the participants indicate that they are aware that the organisation is committed to the protection of personal information, and they know how to identify personal information and sensitive personal information. The rest of the top ten statements indicate that the participants are aware of the consequences of a privacy breach and the importance of privacy training as well as that the organisation is committed to ensure that each employee understands the importance of protecting personal information.

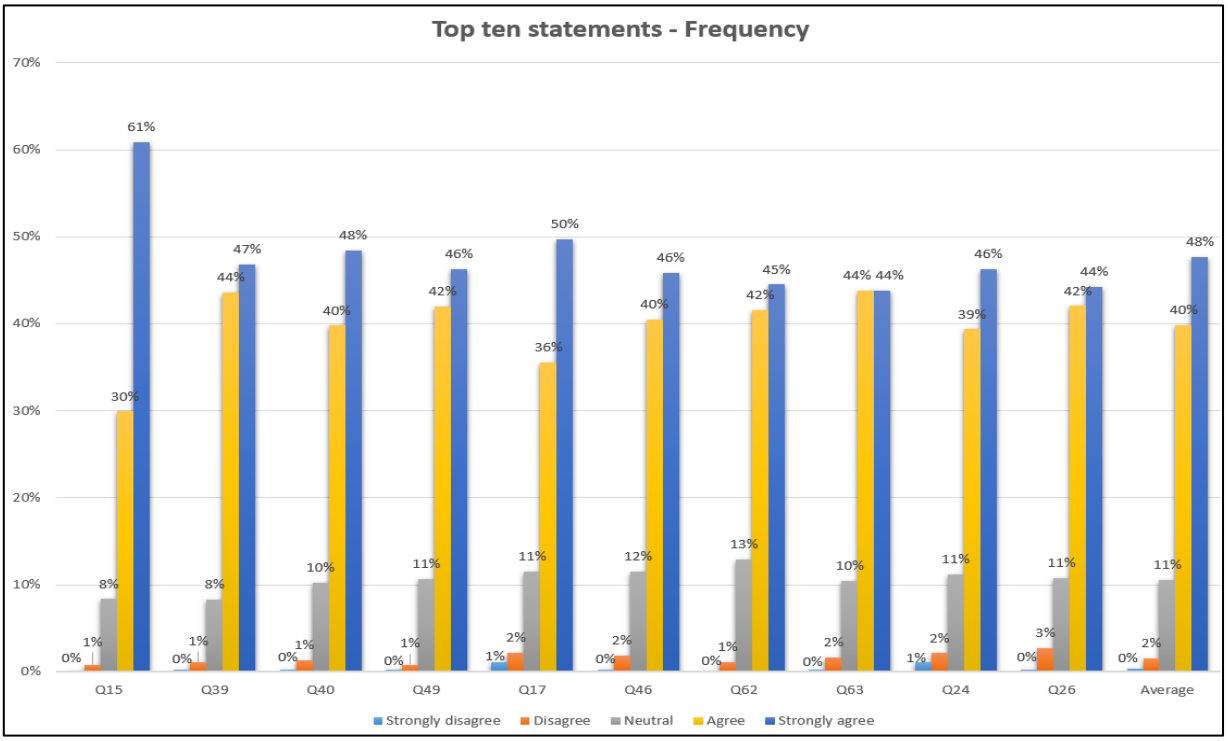


Figure 5-13: Top ten statements - Frequencies (Likert scale)

Figure 5-14 below shows the bottom ten statements with the lowest mean values. The average frequencies for *strongly agree* is 35%, *agree* is 38%, *neutral* is 20%, *disagree* is 6% and *strongly disagree* is 1%. For the *strongly agree* and *agree* scales, the frequencies are distributed evenly, and the *neutral* scale is higher than the *neutral* scale for the top ten statements.

The bottom ten statements fall into the following dimension categories: *Leadership Commitment, Privacy Office, Reporting, Information Officer, Communication, Breach Handling / Incident Management, Privacy Awareness and Training* and lastly, *Ongoing Assessment and Evaluation*. Question 20, which has the lowest mean value, shows that respondents are not encouraged to interact with the Information Officer for important business decisions. Questions 30, 56 and 60, where the mean values are below 4, indicate that the reporting structures to report a privacy matter are not clear, notification regarding a privacy breach or incident and customisation of privacy training are both concerns for the employees. The rest of the bottom ten statements indicate that almost a third of the participants are either neutral or disagree with the organisation's commitment regarding the implementation of regulatory requirements, timeframe to report a personal data compromise, notification of privacy rights, privacy practice updates, and lastly the role of the Privacy Office.

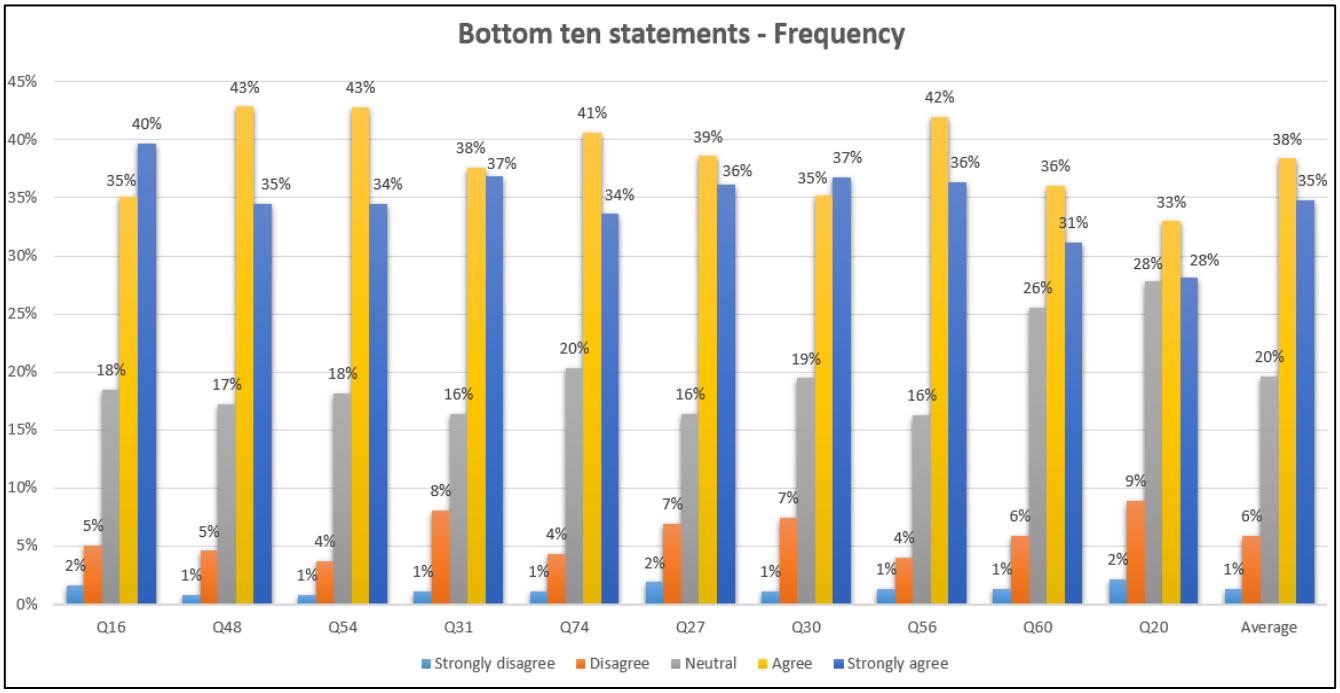


Figure 5-14: Bottom ten statements - Frequencies (Likert scale)

5.3 Validation of the instrument

In the following sections, the EFA will be discussed as well as determining the underlying factors of the questionnaire.

To test the validity of the constructs in the questionnaire, the norm for the sample size of 5:1 suggested by Burns and Burns (2008) implies that five times as many respondents as the number of questions are required to have a statistically viable sample. The questionnaire consists of 60 statements, excluding the six biographical questions, which give a total of 300 responses needed for this survey to comply with the suggestion above. At closing of the online survey, a total of 377 useable responses have been received which is an adequate sample to proceed with the validity analysis.

The data were collected and analysed statistically with the support of a qualified statistician. The SPSS Version 25 software package was used to analyse the data statistically. To test the validity, the EFA statistical technique was employed to detect hidden structures and to enhance the interpretability of the data (Treiblmaier & Filzmoser, 2010), and thus, to determine construct validity.

Prior to conducting the EFA, the adequacy of the correlation matrices for factor analysis, using the Kaiser-Meyer-Olkin (KMO) test and the Bartlett sphericity test (Treiblmaier & Filzmoser, 2010), were investigated. A KMO greater than 0.8 shows good sampling adequacy and a KMO greater than 0.9 shows excellent sampling adequacy (Sreejesh et al., 2014). The KMO value of 0.964, as indicated in Table 5-3, shows that the sampling adequacy is excellent to conduct the EFA. The Bartlett sphericity test, where the probability should be 0.05 or less, was statistically significant ($p < 0.000$) which meant that the variables were correlated highly enough to conduct the EFA (Sreejesh et al., 2014). The results of the Bartlett sphericity test are portrayed in Table 5-3. With this confirmation, the researcher was able to continue with the factor analysis and to identify the underlying factors.

Table 5-3: KMO and Bartlett's sphericity tests

Kaiser-Meyer-Olkin Measure of Sampling Adequacy		0.964
Bartlett's Sphericity Test	Approx. Chi-Square	19813.574
	df	1770
	Sig.	0.000

5.3.1 Determining the number of factors

In determining the underlying factors for the variables, the initial Eigenvalues (refer to Table 5-4 below) and the scree plot (see Figure 5-15) were utilised as well as the cumulative percentage (Gerber & Hall, 2017). The factors should have an Eigenvalue greater than one (Kaiser, 1960) to ensure an internal consistency. For this study, the Eigenvalues for four factors were larger than 1 which suggested that four factors might be extracted (Treiblmaier & Filzmoser, 2010) with a cumulative Eigenvalue of 74.4%.

Table 5-4: Eigenvalues for factors

Total Variance Explained				
Factor	Initial Eigenvalues			Rotation Sums of Squared Loadings
	Total	% of Variance	Cumulative %	Total
1	39.461	65.768	65.768	35.284
2	1.966	3.277	69.045	26.015
3	1.714	2.857	71.902	20.666
4	1.502	2.504	74.406	27.335

The scree plot is a graph plotting the Eigenvalues on the y-axis and used to determine the number of meaningful factors. The scree plot has a sharp descent, and it is at the turning point where the graph levels out which indicates the cut-off for the meaningful

factors (Gerber & Hall, 2017). The cut-off for the number of factors on the scree plot (refer to Figure 5-15) is four factors.

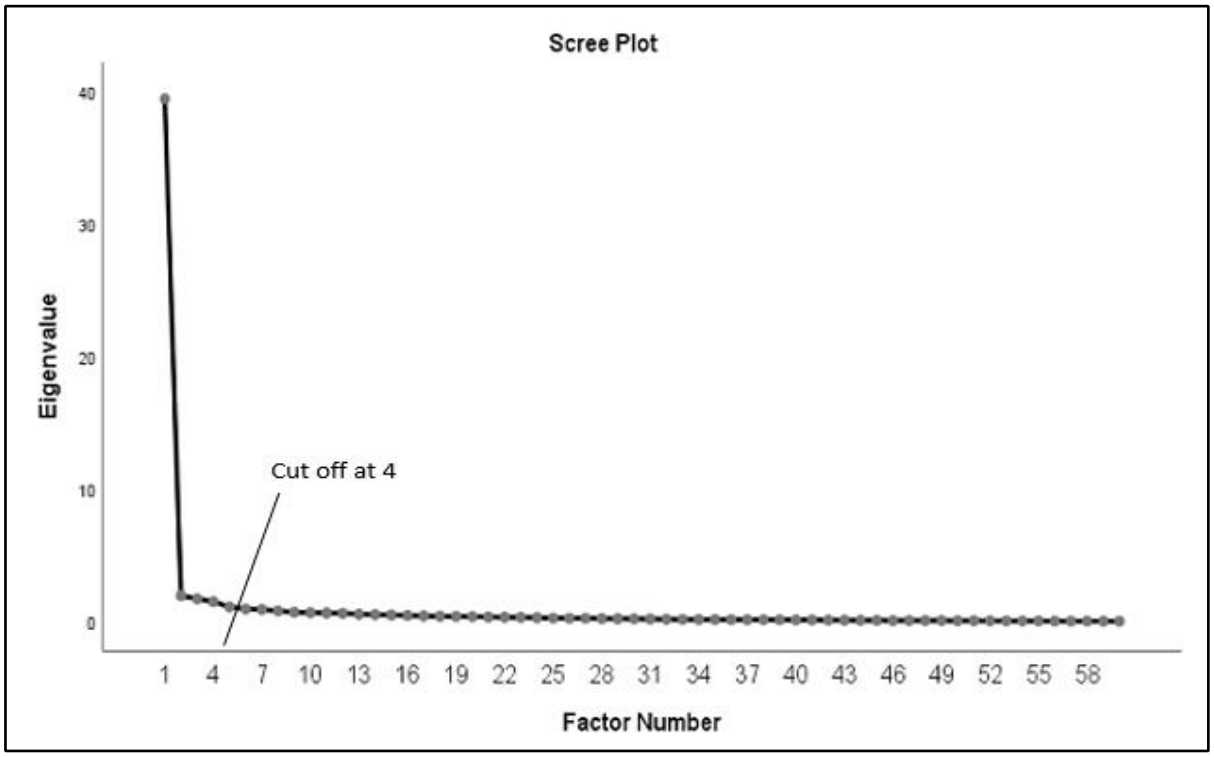


Figure 5-15: Scree plot (Source: Calculated from survey results)

After inspecting the communalities (Appendix I) of the individual items to determine if they should form part of the overall scale. It was determined that the communalities for this study are all above the proposed 0.40 and none of the statements will be reconsidered, as they associate well with one another (Gerber & Hall, 2017; Hair, Anderson, Babin & Black, 2010).

After scrutinising the Eigenvalues and the scree plot, four factors have been extracted, explaining cumulative percentage of 74.406% (refer to Table 5-4 above). This is sufficient to continue with the factor analysis, as the cumulative percentage should be higher than 60% (Hair et al., 2010). According to this guideline, either two (69.05%) or even three (71.90%) factors may be extracted, but it makes statistical sense to extract four factors, as the Eigenvalue for the fourth factor is greater than one, and another 3% of the variance can be explained when extracting four factors.

Given the above, the next step was the EFA. A principle axis extraction was consequently applied using a Direct Oblimin rotation. The Oblimin rotation was

chosen, as it accommodated correlated factors (Burns & Burns, 2008), and it also provided good and meaningful interpretation of the factors (Sreejesh et al., 2014). Table 5-5 displays the four rotated factors and the factor loadings. Factor loadings are used to determine the composition of the factors (Gerber & Hall, 2017). A loading of more than 0.4 is considered meaningful when loading on a specific factor.

After the final PAF, the questionnaire items and corresponding loadings are listed in Table 5-6. For cross loadings on more than one factor, the highest loading has been kept as part of that specific factor and after taking note of the theory behind the factors. Question 44 in Table 5-5, indicated with the blue highlighting, has a cross loading on factors 1 and 2 respectively, but the loading is reconsidered to be part of factor 2 (0.491). Question 29 in Table 5-5, indicated with the blue highlighting, is part of factor 3, as it loads higher (0.480) on factor 3.

Table 5-5: Rotated pattern matrix

Question	Factor				Question	Factor			
	1	2	3	4		1	2	3	4
67	0.862				40		0.885		
68	0.861				39		0.863		
72	0.851				42		0.799		
74	0.826				49		0.671		
71	0.822				41		0.538		
69	0.811				46		0.496		
70	0.807				44	0.435	0.491		
73	0.783				51	0.363	0.416		
65	0.771				31			0.584	
53	0.725				30			0.577	0.371
56	0.723				27			0.524	
59	0.715				48			0.500	
64	0.692				29			0.480	0.419
66	0.629			0.339	35			0.411	
50	0.622				15				0.816
57	0.611				25				0.720
54	0.597		0.345		17				0.691
60	0.580				24				0.689
58	0.549				23				0.631
52	0.528				21				0.544
37	0.499				22				0.472
61	0.465				18				0.442
55	0.465				26				0.401
43.	0.447								
28	0.416								
47	0.406								

Extraction Method: Principal Axis Factoring. Rotation Method: Oblimin with Kaiser Normalisation.

Table 5-6: Factor loadings

Factor 1	
Question	**Factor Loading**
67	0.862
68	0.861
72	0.851
74	0.826
71	0.822
69	0.811
70	0.807
73	0.783
65	0.771
53	0.725
56	0.723
59	0.715
64	0.692
66	0.629
50	0.622
57	0.611
54	0.597
60	0.580
58	0.549
52	0.528
37	0.499
61	0.465
55	0.465
43	0.447
28	0.416
47	0.406

Factor 2	
Question	**Factor Loading**
40	0.885
39	0.863
42	0.799
49	0.671
41	0.538
46	0.496
44	0.491
51	0.416

Factor 3	
Question	**Factor Loading**
31	0.584
30	0.577
27	0.524
48	0.500
29	0.480
35	0.411

Factor 4	
Question	**Factor Loading**
15	0.816
25	0.720
17	0.691
24	0.689
23	0.631
21	0.544
22	0.472
18	0.442
26	0.401

The rotated factor matrix provides clarity and simplicity of factor loadings (Osborne, 2015). Referring to Table 5.6, twenty-six (26) items were found to load on the first factor which was labelled as *Privacy controls assessment*. For factor 2, eight items loaded. It was labelled as *Personal information awareness and assessment*. Six items loaded on the third factor which was labelled as *Privacy governance reporting*. For the fourth factor, nine items loaded and it was labelled as *Organisational commitment.*

Given the discussion of the constructs for privacy, the four factors also make theoretical sense.

5.4 Testing reliability of the factors dimensions

To test the reliability of the four factors from EFA, reliability analysis was conducted, calculating the Cronbach Alpha coefficient. Reliability means consistency or dependability, and that under similar conditions the same thing can be recreated (Neuman, 2014).

Gerber and Hall (2018) provide criteria to interpret the Cronbach Alpha coefficient as follows:

- A good reliability is considered for a value above 0.8.
- An acceptable reliability is considered for values between 0.6 and 0.8.
- An unacceptable reliability is considered for a value less than 0.6.

The results of the Cronbach's Alpha are portrayed in Table 5-7.

The Cronbach Alpha was used to measure the internal consistency of the four factors, and the overall reliability coefficient for all four factors was above 0.8 as reported in Table 5-7. Only one item (Q18) would increase the reliability coefficient to 0.953 (overall coefficient for factor 4 is 0.950) if it were discarded. After considering the *Corrected item – Total correlations* (0.679) column for Q18, it was considered to maintain the item because the *Corrected item – Total correlation* should not be less than 0.4 (Mattick & Clarke, 1998). There is a marginal difference between the overall Cronbach Alpha for factor 4 and the *Cronbach's Alpha if Item Deleted* criterion. All the

items were maintained because if an item was deleted, the Cronbach Alpha was still above 0.8 which was considered a good reliability (Appendix J).

Table 5-7: Cronbach Alpha coefficient values for the survey variables

Subscale	Factors	Items	No. of items	Items omitted	Cronbach Alpha	Reliability
	Privacy controls assessment	67, 68, 72, 74, 71, 69, 70, 73, 65, 53, 56, 59, 64, 66, 50, 57, 54, 60, 58, 52, 37, 61, 55, 43, 28, 47		None	0.984	Good
	Personal information awareness and assessment	40, 39, 42, 49, 41, 46, 44, 51		None	0.947	Good
	Privacy governance reporting	31, 30, 27, 48, 29, 35		None	0.940	Good
	Organisational commitment	15, 25, 17, 24, 23, 21, 22, 18, 26		None	0.950	Good
Overall	**Factors**			**None**	**0.955**	**Good**

The overall Cronbach Alpha was 0.955, and the estimates were between 0.940 and 0.984. These results for the constructs indicated a good internal consistency, as per the criteria above for the Cronbach Alpha.

5.5 Comparison of demographic groups

After analysing the data by means of EFA and determining the number of factors underlying the dataset, the information of the factors was used to determine how factor scores differed among groups (Distefano, Zhu & Mîndrilă, 2009). ANOVA is a method used to test the “equality of means amongst multiple samples” (Van den Honert, 1999:21). ANOVA was conducted for each factor and biographical variable (Appendix H). For the post hoc tests, Scheffé’s method was used to identify which pairs of means differed significantly from one another (Van den Honert, 1999:39).

A significance level of 0.05 was used for both the ANOVA and Scheffé tests (Cooper & Schindler, 2014). The questionnaire consisted of six biographical statements (age; gender; employment status; job level; length of service; and business unit).

The results of the statistical data show that there are only three significant differences between the means of the biographical groups, namely age and two significant differences in the employment status group. Only the results of the biographical groups with significant differences will be discussed in the following sections.

5.5.1 Relationship between the age criterion and the factors

The results of the ANOVA for comparing age groups on the four factors are presented in Table 5-8. The privacy controls assessment factor shows a significant difference between age groups F = 4.506 (p = 0.012). The significance values of the other three

Table 5-8: ANOVA: Age groups

ANOVA							Descriptive			
		Sum of Squares	df	Mean Square	F	Sig.	Age Groups	Mean	Std Dev.	Std Error
Privacy controls assessment	Between Groups	4.262	2	2.131	4.506	**0.012***	1946-1964	4.0320	0.67663	0.10201
	Within Groups	175.916	372	0.473			1965-1980	3.9850	0.70839	0.06785
	Total	180.177	374				1980-2000	4.2137	0.67948	0.67948
Personal information awareness assessment	Between Groups	2.231	2	1.115	2.707	0.068	1946-1964	4.2955	0.70044	0.10560
	Within Groups	153.304	372	0.412			1965-1980	4.1379	0.67462	0.06462
	Total	155.535	374				1980-2000	4.3098	0.61304	0.04114
Privacy governance reporting	Between Groups	2.428	2	1.214	1.898	0.151	1946-1964	4.0000	0.86714	0.13073
	Within Groups	237.895	372	0.640			1965-1980	3.9394	0.80683	0.07728
	Total	240.323	374				1980-2000	4.1167	0.78232	0.05251
Organisational commitment	Between Groups	1.293	2	0.646	1.281	0.279	1946-1964	4.2778	0.73566	0.11091
	Within Groups	187.728	372	0.505			1965-1980	4.1529	0.76156	0.07294
	Total	189.021	374				1980-2000	4.2830	0.67876	0.04556

factors are above 0.05, and therefore, there is no significant difference between the age groups on any of these factors. To explore the nature of the t differences between the age groups on the *Privacy controls assessment* factor, the post hoc test was conducted with a multiple comparisons table presented in Table 5-9 below. (Also see Appendix H for detailed results.)

Table 5-9: Post hoc test: Age group for the Privacy controls assessment factor

Multiple Comparisons

Scheffé

Dependent Variable			Mean	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
							Lower Bound	Upper Bound
Privacy controls assessment	1946-1964 (Mean: 4.0320)	1965-1980	3.9850	0.04696	0.12283	0.930	-0.2549	0.3488
		1981-2000	4.2137	-0.18169	0.11348	0.279	-0.4606	0.0972
	1965-1980 (Mean: 3.9850)	1946-1964	4.0320	-0.04696	0.12283	0.930	-0.3488	0.2549
		1981-2000	4.2137	-.22865*	0.08043	**0.018***	-0.4263	-0.0310
	1981-2000 (Mean: 4.237)	1946-1964	4.0320	0.18169	0.11348	0.279	-0.0972	0.4606
		1965-1980	3.9850	.22865*	0.08043	**0.018***	0.0310	0.4263

*. The mean difference is significant at the 0.05 level.
Source: Calculated from statistical data

The results for the age biographical group between 1965-1980 and 1981-2000 show a significant difference. It is evident from the means in Table 5-8 that the age group 1965-1980 (mean: 3.98) scored significantly lower than the group (1981-2000, mean: 4.21) which meant they were less positive regarding the privacy management controls than the other groups. This was confirmed by Close and Martins (2015) where Generation Y have a more positive attitude, personal ambition and goals and an increased self-confidence. Generation Y is also constantly exposed to information and communication technologies (Close & Martins, 2015).

The 1965-1980 age group is mostly part of the Generation X group. These are loyal, hardworking individuals who ensure good performance and organisational commitment (Close & Martins, 2015). They focus on organisational values, innovation, autonomy and diversity, and are motivated by integrated work goals (Close & Martins,

2015). The 1981-2000 age group is part of the Millennials generation group. The Millennials group is diverse, entrepreneurial-minded, goal-driven, success-driven, technologically savvy and highly educated (Moss, 2014).

The South African perspective on Generation Y employees is that they are good in systems thinking and more counter-intuitive and learning-oriented (Moss, 2014). The mean difference between the two groups shows that the 1981-2000 age group is more positive than the 1965-1980 age group towards the *Privacy controls assessment* variables.

A study done by Moss (2014) shows that Generation Y employees are more positive than Generation X employees regarding strategy and change management, as they have a stronger external locus of control. The difference between these two age groups could relate to the 1965-1980 age group being performance-driven and loyal to their leadership, while the 1981-2000 age group is open-minded, technology savvy and highly educated. To be a productive team, only awareness and understanding of the privacy programme controls can reduce stress to work together effectively (Kicheva, 2017). They are the ones who understand the business policies, processes and privacy controls to make informed decisions.

5.5.2 The relationship between employment status groups on the factors

The results of the ANOVA for *Employment status* groups are presented in Table 5-10.

The *Privacy controls assessment* factor shows a significant difference between the two *Employment status* groups F = 4.210 (p = 0.041). The mean differences of the permanent (4.07) and contractor/vendor (4.24) variables show that the contractors/vendor group perception is significantly more positive regarding the privacy controls that are in place within the organisation.

Table 5-10: One-way ANOVA: Employment status

ANOVA							Descriptive			
		Sum of Squares	df	Mean Square	F	Sig.	Employment Status	Mean	Std. Dev.	Std. Error
Privacy controls assessment	Between Groups	2.006	1	2.006	4.210	**0.041***	Permanent	4.0782	0.7055	0.04294
	Within Groups	177.721	373	0.476			Contract / Vendor	4.2410	0.64918	0.06335
	Total	179.727	374							
Personal information awareness assessment	Between Groups	1.206	1	1.206	2.913	0.089	Permanent	4.2225	0.64832	0.03946
	Within Groups	154.343	373	0.414			Contract / Vendor	4.3488	0.62999	0.06148
	Total	155.549	374							
Privacy governance reporting	Between Groups	2.262	1	2.262	3.546	0.060	Permanent	4.0026	0.80042	0.04871
	Within Groups	237.884	373	0.638			Contract / Vendor	4.1756	0.79386	0.07747
	Total	240.146	374							
Organisational commitment	Between Groups	2.843	1	2.843	5.695	**0.018***	Permanent	4.1906	0.72341	0.04403
	Within Groups	186.234	373	0.499			Contract / Vendor	4.3845	0.66116	0.06452
	Total	189.077	374							
*. The mean difference is significant at the 0.05 level										

There is also a significant difference between the permanent and contractor/vendor groups for the *Organisational commitment* factor F = 5.695 (p = 0.018), as per Table 5-10 above. The mean difference of the permanent (4.19) and contractor/vendor (4.38) variables shows that the contractor/vendor group's perception is significantly more positive regarding the leadership commitment towards the implementation of privacy controls, policies and procedures within the organisation. The overall results for the *Employment status* group show that the mean of the contractor/vendor group is more positive than that of the permanent staff regarding *Privacy control assessment* and *Organisational commitment*. Contractors or vendor employees have to abide by the privacy policies and procedures of their own organisations and those of the financial institution to which they are assigned to deliver a service. A study done by Ang and Slaughter (2006) shows that there is a difference between employee perceptions of temporary and permanent employees, and that temporary employees perceive their work environment more positively. According to Giunchi, Chambel and Ghislieri (2014), contract employees have a double employment relationship and also have affective commitment towards the client organisations.

This view is supported by a study done by Van Breugel, Van Olffen and Olie (2005) who have found that affective commitment towards the organisation by contract workers is more positive due to the support by the agency and the client organisation. Contract employees are, therefore, encouraged by the agency and the client organisation to comply with their respective privacy policies and procedures in order to protect the personal information that they process.

5.6 Chapter summary

The general aim of this research study is to develop a CPGF that can be used to develop a valid and reliable IPGQ to assess the perception of employees on how effective the organisation governs privacy. This chapter addressed the first two empirical research questions regarding the validity and reliability of the questionnaire and the perception of how effective the organisation governs privacy. The second empirical research question is a preparation for the third empirical research question to make recommendations to propose improvements for the governing of privacy within the organisation.

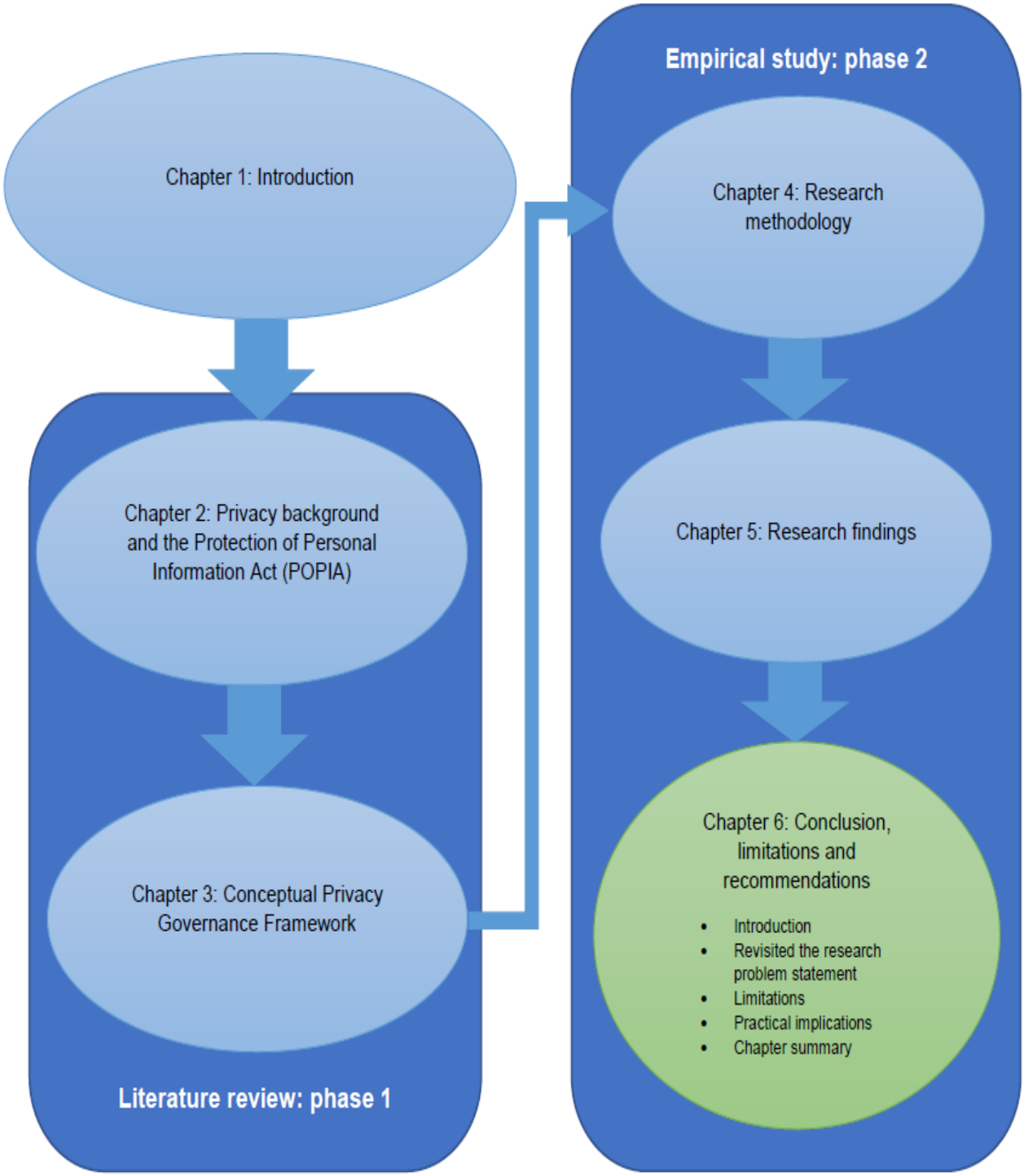
The questionnaire was tested in a South African financial institution, and the data collected were available to the researcher to test the validity and internal reliability of the constructs. EFA was used to determine the underlying factorial structure and the Cronbach Alpha was used to establish the internal reliability of the factors.

From the initial item reduction of the constructs, four factors were derived to test the privacy perception of employees, namely:

- Factor 1 - *Privacy Controls Assessment* using twenty-six items.
- Factor 2 - *Personal Information Awareness and Assessment* using eight items.
- Factor 3 - *Privacy Governance Reporting* using six items.
- Factor 4 - *Organisational Commitment* using nine items.

In the following chapter, the conclusion and recommendations regarding the outcomes of this research study will be discussed.

CHAPTER 6


Chapter 1: Introduction
Chapter 2: Privacy background and the Protection of Personal Information Act (POPIA)
Chapter 3: Conceptual Privacy Governance Framework
Literature review: phase 1
Empirical study: phase 2
Chapter 4: Research methodology
Chapter 5: Research findings
Chapter 6: Conclusion, limitations and recommendations
Introduction
Revisited the research problem statement
Limitations
Practical implications
Chapter summary

Conclusion, limitations and recommendations

6.1 Introduction

This study addresses the development of the CPGF and the IPGQ to assess the perception of employees of how effective the organisation governs privacy. The CPGF consists of privacy governance components that aid in effective privacy governance at various levels of the organisation, thereby cultivating a certain level of a privacy culture. The IPGQ instrument, which is based on the CPGF, has been developed in this study. It is used to measure the perception of employees in a financial organisation to validate and to determine how effective the organisation governs privacy.

The purpose of this chapter is to review the extent to which the literature review and empirical research questions have been addressed. The remaining sections will discuss the recommendations for the organisation, the limitations of the study and recommendations for future research studies.

6.2 Revisited the research problem statement

The general aim of this research is to develop the conceptual privacy governance framework that can be used to develop a valid and reliable IPGQ to assess the perception of employees of how effective the organisation governs privacy. The research questions are answered in the following section.

6.2.1 Conclusion for research aims regarding literature review

Research aim 1: To develop a comprehensive privacy governance framework from a theoretical perspective

Chapter 2 provided the background to privacy and the rationale for the implementation of the POPIA. The conditions of the POPIA as well as the purpose of the Act were discussed for the lawful processing and protection of personal information. These conditions and purpose of the Act should be incorporated in the privacy policies, procedures and controls of what the organisation should implement to comply with the

privacy law of the country. To effectively govern the implementation of the POPIA, organisations require guidance such as a privacy framework.

To answer the research question, chapter 3 discussed and compared current privacy governance frameworks and contributions made by Herold (2005), Delgado (2011), Weber (2014) and Seerden et al. (2018) to conceptualise a privacy governance framework for the South African financial organisations.

The CPGF is comprehensive and involves people, policies and processes, privacy programme controls and the ongoing evaluation of the policies, processes and controls. The four main components of the framework are *Organisational Commitment*, *Privacy Policies and Procedures*, *Privacy Programme Controls* and *Ongoing Assessment and Review*.

Such a framework can help management to understand what privacy governance entails and to enable them to implement the required privacy governance framework components to ensure that the employees understand and adhere to the privacy policies, procedures and privacy programme controls, herewith aiding the organisation to implement privacy governance with the objective of effectively governing the implementation of the POPIA in the organisation. The CPGF serves as the theoretical input to address content validity for the development of the IPGQ.

The research question was addressed in Chapter 3 whereby the terms corporate, IT and data governance were discussed as background to provide an overview of the components that contribute positively to effective privacy governance in the organisation. The core components of corporate, IT and data governance are *leadership*, *reporting*, *risk governance*, *compliance*, *assurance and evaluation*. These core components are evident in the privacy governance frameworks that have been discussed in Chapter 3.

As depicted in Figure 3-4 and Table 3-6 of Chapter 3, the consolidated list of factors of four existing privacy governance frameworks, including the four articles in the literature review, has been presented. The researcher has used the consolidated list of components to design the CPGF consisting of the following four core components,

namely *Organisational Commitment*, *Privacy Policies and Procedures*, *Privacy Programme Controls* and *Ongoing Assessment and Review*. These four components are then sub-divided into thirteen sub-components, as depicted in Table 6-1 below.

Table 6-1: Summary of factors for effective privacy governance

Organisational commitment	Privacy Policies and Procedures	Privacy Programme Controls	Ongoing Assessment and Review
Leadership Commitment	Privacy Policies and Procedures	Personal Information Inventory	Ongoing Assessments and Evaluation
Information Officer		Breach Handling / Incident Management	
Privacy Office		Service Provider Management	
Reporting		Communication	
		Privacy Awareness and Training	
		Risk Assessment Tools	
		Programme Assurance / Audit	

A summary of each component for effective privacy governance are given below.

6.2.1.1 Organisational Commitment

Leadership Commitment

The first condition of the POPIA legislation is accountability, which the organisation as the responsible party, must act upon when processing personal information. To be accountable, the leadership (senior management) must be committed to ensure that the organisation is compliant with privacy legislation.

Information Officer

Part B of Chapter 5 (Section 55) of the POPIA describes the responsibilities of an Information Officer and deputy Information Officer. The role of the Information Officer is very important for the strategic planning of the business, as well as the assessment and revision of the privacy program.

Privacy Office

The Privacy Office team usually consist of different team members of all areas of the organisation. The main responsibilities of the Privacy Office, identified by the IAPP-EY privacy governance survey, is the development of privacy policies and procedures; privacy awareness and training, privacy breach and incident management; design and implement privacy controls; communication and privacy impact assessment.

Reporting

Principle 5 of the King IV report states that the reports issued by the governing body of the organisation helps the stakeholders to make informed assessments, and also demonstrate that the organisation complies with the relevant laws.

6.2.1.2 Private Policies and Procedures

Privacy Policies and Procedures

Policies and operational plans are developed by management who gives direction regarding privacy strategies, according to the King IV Report, and must be approved by the governing body.

6.2.1.3 Privacy Programme Controls

Personal Information Inventory

The organisation must keep an inventory of the personal information records they process. Therefore, organisations must document and understand the personal information processed and where it is stored.

Breach Handling / Incident Management

Privacy breaches and security incidents can occur due to unauthorised access to data, negligence of employees or malicious and criminal attacks. A procedure for breach handling must be documented clearly and should include five activities, namely (1) detections; (2) escalation, (3) breach handling, (4) breach notification and (5) reporting.

Service Provider Management

Third-party agreements and audit procedures must be in place to ensure compliance with the organisation's privacy policies and procedures. The service provider must comply with the service-level agreement or contract which includes adherence to the organisation's privacy policies.

Communication

Condition 6 of the POPIA requires the responsible party to be open and transparent. Organisations have a responsibility to inform individuals of their privacy rights by means of privacy notices on their websites and social media and through mobile communication.

Privacy Awareness and Training

Privacy training must be conducted annually to assess the employees' understanding of the privacy policies and procedures as well as to update employees of any new changes to these policies and procedures.

Risk Assessment Tools

Privacy-impact assessments can assist organisations in mitigating and identifying security risks and leakages. Risk assessment procedures must be in place to assess, identify and manage privacy risk.

Programme Assurance / Audit

Organisations must ensure that internal and external audits are conducted to monitor compliance with their privacy policies. To improve the privacy processes, internal audits need to be conducted to identify areas of improvement as well as privacy self-assessments which are conducted by the business units.

6.2.1.4 Ongoing Assessment and Review

Ongoing Assessments and Evaluation

An oversight and review plan must be implemented by the Privacy Officer to ensure the privacy management programme is monitored and assessed effectively. The objective of the review plan is to ensure that the privacy operations are executed in alignment with the defined privacy processes. Privacy controls must be evaluated and

updated on a regular basis. These controls are the policies and procedures; personal information inventory, privacy awareness and training; breach and incident management; communication; and service provider management.

Research aim 2: To conceptualise the dimensions and items of an information privacy governance questionnaire

Chapter 3 discusses the components of the developed CPGF and theoretical statements which provide the basis for the IPGQ statements. The CPGF consists of thirteen sub-components while three to five theoretical statements have been derived from the theory based on the CPGF in Chapter 3. For each theoretical statement, one to three questionnaire statements have been derived. These have been used to measure the privacy perception of the employees of how effective the organisation governs privacy.

The IPGQ consists of the sections, namely Section 1: Biographical information; Section 2: General awareness; and Section 3: Privacy governance perception. Section 1 consists of six questions with regard to age, gender, employment status, length of service, job level and business unit. Section 2 consists of eight questions to determine the participants' knowledge about the privacy policies and procedures within the organisation. Section 3 consists of 60 questions that are based on the theoretical statements of the CPGF. The questions in Section 3 are grouped together according to the sub-components of the CPGF, and range from three to seven questions per sub-section.

6.2.2 Conclusion for research aims regarding the empirical research

Research aim 1: To determine the validity and reliability of the Information Privacy Governance Questionnaire (IPGQ)

The IPGQ measurement instrument designed in Chapter 4 was derived from the theoretical statements of the CPGF. Content validity of the measurement instrument was ensured by comparing the questionnaire statements with the theoretical statements of the CPGF theory. Furthermore, the face validity of the questionnaire statements was validated by the expert panel and pilot group who assessed the questions for understandability, clarity and relevance to the field of study.

To ensure validity and reliability of the assessment instrument, the instrument was tested statistically by using data from the empirical study. The construct validity, which was discussed in Chapter 5 for the empirical research study, proved that the variables were correlated and that they associated well with one another. The validity of the assessment instrument was tested by considering the factor analysis acceptance criteria. All the requirements were met in this respect. The reliability of the assessment instrument was confirmed by the empirical data analysis, since all the statement internal consistencies were higher than those of the minimum requirements. The range of the Cronbach Alpha was 0.940 – 0.984 which presented a good reliability. The statements of the IPGQ assessment instrument and the way in which the statements were grouped could be accepted theoretically and statistically.

Research aim 2: To determine the perceptions of employees in terms of how effective the organisation governs privacy

The overall perceptions of the participants of the organisation were very positive regarding the governance of privacy within the organisation. The knowledge questions that were asked (refer to Section 5.2.2) showed that most of the employees agreed that they had completed their mandatory privacy compliance test and had read the data privacy policies of the organisation. Concerns that were raised during the survey were that employees were not aware of the contact details of the Privacy Office or who the Privacy Officer of the organisation was, something on which the organisation could improve. A privacy governance survey done by PricewaterhouseCoopers (PwC) in 2017 showed that the general awareness of employees was still a point of concern, and that there was a strong need for periodic training and awareness campaigns (PricewaterhouseCoopers, 2017).

The demographical age groups also showed a significant difference between the Generation X (1965-1980) and the Generation Y (1981-2000) employees. The Generation Y group of employees was more positive towards the privacy programme controls that had been implemented throughout the organisation. The theory showed that the Generation Y group was more open-minded, technology savvy and highly

educated, and understood the business policies, processes and privacy programme controls in order for them to make informed decisions.

The statistical results showed that there was a significant difference between the permanent employees and contractors/vendors. These overall statistical results indicated that there was a perception that contractors/vendors adhered to the privacy policies, procedures and privacy programme controls as per their contractual agreement with the organisation, and that the permanent employees did to a lesser extent.

A study done by Ang and Slaughter (2006) shows that there is a difference between employee perceptions of temporary and permanent employees, and that temporary employees perceive their work environment more positively. This is an indication that permanent employees must be held more accountable regarding the protection of personal information within the organisation, and be more committed to the implementation of policies, procedures and privacy programme controls.

Research aim 3: To suggest recommendations for the improvement of privacy governance in the organisation

6.2.3 Recommendations for the organisation

Section 1: Biographical group questions

The biographical group results show that there are significant differences between the age groups and two significant differences in the employment status group. Generation X employees must be encouraged to be more accepting of the privacy programme controls. The theory shows that they are hardworking, loyal and performance-driven individuals. They are an asset to the organisation but they must be encouraged to comply with the privacy programme controls which the organisation has implemented. To be a productive team, only awareness and understanding of the privacy programme controls can reduce stress to work together effectively (Kicheva, 2017). The mean score of the permanent employees is lower than that of the contractors/vendors regarding organisational commitment and privacy controls.

According to Giunchi et al. (2014), contract employees have a double employment relationship and show affective commitment towards the organisation.

Section 2: General awareness questions

The knowledge questions reveal that the organisation must improve on its communication to ensure each employee knows who the Information Officer is and what the contact details of the Privacy Office and its leadership structure are. An awareness campaign may be launched whereby the organisation communicates the information on its intranet or by means of a newsletter.

Another concern raised, shows that the organisation needs to improve on its scheduling of annual training sessions for all employees. This annual privacy training will ensure that all employees are aware of any changes in the privacy policies and privacy programme controls.

Section 3: Privacy perception questions

It is evident from the results that permanent employees should be aware of the impact which non-compliance with the protection of personal information may have on the organisation, since the organisation is liable for fines for any breach of the POPIA. Therefore, the organisation must improve on the promotion of privacy training and ensure that a privacy culture is improved within the organisation.

Open statements of the survey show that employees are aware of the seriousness of protecting personal information but they have indicated that managers must encourage employees to adhere to privacy compliance. This can be done by communicating relevant privacy policies and procedures to colleagues in a newsletter or with stand-up meetings of how it effects their daily tasks and the impact non-compliance has on the organisation.

The participants have also indicated that it is not just enough to complete the privacy compliance test but that it must be explained well to everyone to understand privacy and the protection of personal information. Privacy awareness can be communicated well by means of different types of media and art to portray the privacy message to

employees to adhere to policies and procedures. Therefore, privacy training must be coordinated well and presented to each employee to understand his or her role in protecting personal information.

6.2.4 Recommendations for future research

Recommendations and improvement of areas for future research have become evident during the analysis of the statistical results. Recommendations for future research are as follows:

- Follow-up surveys can be done for comparison in the same organisation.
- The questionnaire can be used by other organisations to assess if privacy is governed effectively.
- The survey can be repeated across industries for comparison to aid South African organisations in governing privacy to meet the requirements of the POPIA.
- The questionnaire can then also be further validated across industries.
- The CPGF and IPGQ can be used by the Information Privacy Officers of organisations to firstly, implement privacy governance tasks, assign roles and responsibilities to these, and secondly, to measure their progress against the governing of privacy using IPGQ.
- Academia can further use the questionnaire to validate the framework by using structural equation modelling and to extent the research methodology by incorporating qualitative assessments to assess the effectiveness of information privacy governance in an organisation.

The next section discusses the limitations of the literature review and the empirical research of the research study.

6.3 Limitations

6.3.1 Limitations of the literature review

The POPIA is a new Act which has been promulgated in 2013 while the Information Regulator has been established in 2016. Therefore, organisations are in the process of aligning their privacy policies and procedures with the new Act. In the South African

context, there is no literature about the effective governing of privacy, and from a global perspective, there is also a lack of academic literature.

The privacy governance frameworks were sourced from the Information Regulator websites of the specific countries discussed in Chapter 3. These limitations highlighted the lack of research done in South Africa regarding the development of a privacy governance framework and measuring the effectiveness of privacy governance in organisations. Therefore, the framework was adapted to the South African context and not developed from an existing South African privacy governance framework.

6.3.2 Limitations of the empirical research

One of the potential empirical research limitations for this study is that the researcher has selected a single organisation; therefore, when generalising the results, caution must be taken. Participants from different departments was used within the financial South African organisation to minimise this limitation. Unlike smaller organisations, the large South African financial organisation has a vast number of employees working for it. The processing of personal information and its privacy policies will differ from those of smaller organisations.

Great caution needs to be taken when generalising the results with smaller organisations or other sectors across the country or other global organisations. The reason is that the research study has only been conducted at one financial institution. The data are very positive and the possible reason is that the financial institution have started implementing privacy protection policies and procedures about ten years ago.

The study is not representative of the entire organisation. Participants have been selected from various departments within the financial organisation. A more diverse sample of participants from different departments is necessary for a total representation of the total population.

In the next section, practical implications for future research are discussed.

6.4 Practical implications

Recommendations may prove useful to organisations wishing to improve their privacy policies, privacy programme controls, privacy reporting and organisational commitment.

From the results of this research study, practical implications include the following:

6.4.1 Participant organisation

- Communication and awareness privacy training are two aspects necessary to inform the employees who the Information Officer of the organisation is and what the contact details of the Privacy Office are.
- A privacy culture needs to be instilled into the behaviour of permanent employees to ensure that they comply with privacy policies and procedures. The leadership of the organisation must communicate the consequences of non-compliance with the privacy policies, procedures and the POPIA as well as the impact it has on the organisation and the employees.
- Organisations must consider the generation differences among employees and develop their privacy programme controls accordingly to ensure the efficient governing of privacy.

6.4.2 Academic

- It will be interesting to conduct the study over time and cross-sectional to compare changes in employee perceptions over time because the POPIA has not been implemented fully, and organisations have one year to ensure that they are fully compliant once the POPIA commences.
- The research study should be conducted across different departments of the financial organisation as well as across different organisations to encompass a more diverse research sample.

6.4.3 Industry

- The industry must adapt the CPGF according to its business strategies, policies and procedures.
- The CPGF and IPGQ can be utilised by all industries.

6.5 Chapter summary

The conclusions of the literature review and empirical study were discussed to emphasise the achievements of the specific research aims discussed in Chapter 1. Conclusions regarding the CPGF, components for effectively contributing to privacy governance and the development of the IPGQ were also discussed. Conclusions pertaining to the empirical study related to determining the validity and reliability of the IPGQ measurement tool, perceptions of employees of how effective privacy was governed as well as the recommendations for the improvement of governing privacy in the organisation were all matters receiving close scrutiny in this chapter. The limitations and recommendations were examined in order to provide a view to future research in this field of study.

For this study, a CPGF has been developed which highlights the main and sub-components of the framework for the effective governance of privacy. Statements for the questionnaire have been derived from the CPGF to develop the IPGQ which is proven to be statistically reliable and valid for future research.

REFERENCES

Reference style: APA American Psychological Association (6th ed).

AICPA/CICA. (2011). Privacy Maturity Model. Retrieved January 29, 2019, from https://iapp.org/media/pdf/resource_center/aicpa_cica_privacy_maturity_model_final-2011.pdf

AICPA. (2009). Generally Accepted Privacy Principles CPA and CA Practitioner Version. Retrieved January 29, 2019, from https://www.cpacanada.ca/en/business-and-accounting-resources/other-general-business-topics/information-management-and-technology/publications/business-and-organizational-privacy-policy-resources/gapp-in-privacy-policy-development

Allen & Overy. (2018). The EU General Data Protection Regulation is finally agreed. Retrieved January 29, 2019, from http://www.allenovery.com/SiteCollection Documents/Radical changes to European data protection legislation.pdf

Ang, S., & Slaughter, S. A. (2006). Work outcomes and job design for contract versus permanent information systems professionals on software development teams. *Information Systems Outsourcing (Second Edition): Enduring Themes, New Perspectives and Global Challenges*, *25*(3), 403–441. http://doi.org/10.1007/978-3-540-34877-1_15

Arnaldi, S., Quaglio, G., Ladikas, M., O'Kane, H., Karapiperis, T., Srinivas, K. R., & Zhao, Y. (2015). Responsible governance in science and technology policy: Reflections from Europe, China and India. *Technology in Society*, *42*, 81–92. http://doi.org/10.1016/j.techsoc.2015.03.006

Australian Government. (1988). Privacy Act 1988. Retrieved November 14, 2018, from https://www.legislation.gov.au/Details/C2004C06137

Baloyi, N., & Kotze, P. (2017). Are organisations in South Africa ready to comply with personal data protection or privacy legislation and regulations? *2017 IST-Africa Week Conference, IST-Africa 2017*, 1–11. http://doi.org/10.23919/ IST AFRICA

.2017.8102340

Bamberger, K. A., & Mulligan, D. K. (2011). New governance, chief privacy officers, and the corporate management of information privacy in the United States : An initial inquiry. *Law and Policy*, *33*(4), 477–508.

Bange, V., Hann, G., Jeffery, C., & Annereau, S. (2012). An Overview of UK Data Protection Law. Retrieved January 29, 2019, from http://united-kingdom.taylorwessing.com/uploads/tx_siruplawyermanagement/NB_000168_Overview_UK_data_protection_law_WEB.pdf

Banisar, D. (2018). National Comprehensive Data Protection / Privacy Laws and Bills 2018. Retrieved January 29, 2019, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1951416

Bennett, C. J. (2012). The accountability approach to privacy and data protection: assumptions and caveats. In: Guagnin D., Hempel L., Ilten C., Kroener I., Neyland D., & Postigo H. (eds) *Managing Privacy Through Accountability* (pp. 33–48). London: Palgrave Macmillan.

Bevir, M. (2012). *Governance: A very short introduction* (1st ed.).Oxford: Oxford University Press.

Borena, B., Belanger, F., & Ejigu, D. (2015). Information privacy protection practices in Africa : A review through the lens of critical social theory. *2015 48th Hawaii International Conference on System Sciences Information*, 3490–3497. http://doi.org/10.1109/HICSS.2015.420

Botha, J., Eloff, M. M., & Swart, I. (2015). The effects of the PoPI Act on small and medium enterprises in South Africa. *Information Security for South Africa (ISSA)*, (August), 1–8.

Burns, R. B., & Burns, R. A. (2008). *Business Research Methods and Statistics Using SPSS*. London: Sage Publication.

Butin, D., & Le Metayer, D. (2015). A guide to end-to-end privacy accountability. In *Proceedings - 1st International Workshop on Technical and Legal Aspects of Data privacy and Security, Telerise 2015* (pp. 20–25). http://doi.org/10.1109/TELERISE.2015.12

Cahoy, E. (2016). Empirical Research in Education and the Behavioral/Social Sciences. Retrieved June 20, 2016, from http://psu.libguides.com/emp

Chu, H., & Liao, S. (2010). Buying while expecting to sell: The economic psychology of online resale. *Journal of Business Research*, *63*(9–10), 1073–1078. http://doi.org/10.1016/j.jbusres.2009.03.023

Clamp, C. (2017). King III vs King IV - What You Really Need to Know. Retrieved January 29, 2019, from https://www.grantthornton.co.za/globalassets/1.-member-firms/south-africa/pdfs/kingiv_feb17.pdf

Clearwater, A., & Hughes, J. T. (2013). In the beginning . . . An early history of the privacy profession. *Ohio State Law Journal*, *74*(6), 897–921. Retrieved January 29, 2019, from http://ssrn.com/abstract=2411814

Close, D., & Martins, N. (2015). Generational motivation and preferences for reward recognition. *Journal of Governance and Regulation*, *4*(3), 259–270.

Colquhoun, H. L., Levac, D., Brien, K. K. O., Straus, S., Tricco, A. C., Perrier, L., … Moher, D. (2014). Scoping reviews : Time for clarity in definition, methods, and reporting. *Journal of Clinical Epidemiology*, *67*(12), 1291–1294. http://doi.org/10.1016/j.jclinepi.2014.03.013

Community Care Information Management. (2010). Common Privacy Framework CCIM Assessment Projects. Retrieved January 29, 2019, from http://www.centralwestlhin.on.ca/~/media/sites/cw/Documents/ForHSPs/GeneralResources/CCIM_CommonPrivacyFramework_v1,-d-,0_CPF(1) (4).pdf?la=en

Conway, J. M., & Huffcutt, A. I. (2003). A review and evaluation of exploratory factor analysis practices in organizational research. *Organizational Research Methods*, *6*(2), 147–168. http://doi.org/10.1177/1094428103251541

Cooper, D. R., & Schindler, P. S. (2014). *Business Research Methods.* (12th ed.). New

York: McGraw-Hill Irwin.

Creswell, J. W. (2014). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches.* (4th ed.). California: Sage Publication.

Creswell, J. W., & Creswell, J. D. (2017). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches.* (5th ed.). England: Sage Publication.

Da Veiga, A., & Martins, N. (2015). Information security culture and information protection culture: A validated assessment instrument. *Computer Law and Security Review*, *31*(2), 243–256. http://doi.org/10.1016/j.clsr.2015.01.005

Dala, P., & Venter, H. S. (2016). Understanding the level of compliance by South African institutions to the Protection of Personal Information (POPI) Act. *Proceedings of the Annual Conference of the South African Institute of Computer Scientists and Information Technologists*, *13*, 13:1–13:8. http://doi.org/10.1145/2987491.2987506

De Bruyn, M. (2014). The Protection of Personal Information (POPI) Act - Impact on South Africa. *International Business & Economics Research Journal*, *13*(6), 1315–1340.

De Vaus, D. (2013). *Surveys in Social Research.* (6th ed.). Australia: Routledge.

Delgado, M. (2011). The evolution of health care IT : Are current U.S. privacy policies ready for the clouds ? *IEEE World Congress on Services*, (July), 371–378. http://doi.org/10.1109/SERVICES.2011.70

Denham, E. (2015). An Examination of BC Goverment's Privacy Breach Management. Retrieved January 29, 2019, from https://www.oipc.bc.ca/media/16876/oipc-examination-of-bc-governments-privacy-breach-management.pdf

Dennedy, M. F., Fox, J., & Finneran, T. R. (2014). *The Privacy Engineer's Manifesto - Getting from Policy to Code to QA to Value*. New York: Apress Media.

Dickie, J. (2004). Review of the Privacy and Personal Information Protection Act 1998. Retrieved January 29, 2019, from http://www.ipc.nsw.gov.au/sites/default/files/file_manager/sub_ppipareview2004.pdf

Distefano, C., Zhu, M., & Mîndrilă, D. (2009). Understanding and using factor scores: Considerations for the applied researcher. *Practical Assessment, Research & Evaluation*, *14*(20), 1–11. http://doi.org/10.1.1.460.8553

DLA Piper. (2018). DLA Piper Global Data Protection Laws of the World - World Map. Retrieved January 5, 2019, from https://www.dlapiperdataprotection.com/index.html?t=world-map&c=AO

Ernest & Young. (2013). What Happens if We Violate. Retrieved January 29, 2019, from http://www.ey.com/Publication/vwLUAssets/What_happens_if_we_violate_PoPI/$FILE/130522 Privacy Thought Leadership 2.pdf

Ernest & Young. (2014). Privacy Trends 2014: Privacy Protection in the Age of Technology. Retrieved January 29, 2019, from http://www.ey.com/Publication/vwLUAssets/EY_-Privacy_trends_2014:_Privacy_protection_in_the_age_of_technology/$FILE/EY-Insights-on-GRC-Privacy-trends-2014.pdf

Esterhuizen, W., & Martins, N. (2016). The factor structure of a safety leadership assessment tool for the mining industry. *Journal of Contemporary Management*, *13*(1), 1–26.

Etikan, I., Musa, S. A., & Alkassim, R. S. (2016). Comparison of convenience sampling and purposive sampling. *American Journal of Theoretical and Applied Statistics*, *5*(1), 1–4. http://doi.org/10.11648/j.ajtas.20160501.11

Felici, M., & Pearson, S. (2015). Accountability for data governance in the cloud. *Springer International Publishing*, *8937*, 3–42. http://doi.org/10.1007/978-3-319-17199-9

Finn, R. L., Wright, D., & Friedewald, M. (2013). Seven types of privacy. *European Data Protection: Coming of Age*, (January), 3–32. http://doi.org/10.1007/978-94-007-5170-5_1

Fowler Jr, F. J. (2013). *Survey Research Methods*. (5th ed.). California: Sage Publication.

Gellert, R., & Gutwirth, S. (2012). Beyond accountability, the return to privacy? In: Guagnin D., Hempel L., Ilten C., Kroener I., Neyland D., & Postigo H. (eds) *Managing Privacy Through Accountability* (pp. 261–283). London: Palgrave Macmillan.

General Data Protection Regulation (EU). (2016). General Data Protection Regulation (EU) 2016/679. Retrieved June 27, 2017, from http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&qid=1490179745294&from=en

Gerber, H., & Hall, R. (2017). Quantitative research design. In *Data Acquisition - 1 Day* (pp. 30–56). Pretoria: HR Statistics (Pty) Ltd.

Gie Yong, A., & Pearce, S. (2013). A beginner's guide to factor analysis: Focusing on exploratory factor analysis. *Tutorials in Quantitative Methods for Psychology*, *9*(2), 79–94.

Giles, J. (2016). What Does the GDPR Mean for the POPI Act? Retrieved January 29, 2019, from https://www.michalsons.com/blog/gdpr-mean-popi-act/19959

Giunchi, M., Chambel, M. J., & Ghislieri, C. (2014). Contract moderation effects on temporary agency workers' affective organizational commitment and perceptions of support. *Personnel Review*, *44*(1), 22–38. http://doi.org/10.1108/PR-03-2014-0061

Golafshani, N. (2003). Understanding reliability and validity in qualitative research. *The Qualitative Report*, *8*(4), 597–606.

Grant, M. J., Booth, A., & Centre, S. (2009). A typology of reviews : An analysis of 14 review types and associated methodologies. *Health information & libraries journal*, 26(2), 91–108. http://doi.org/10.1111/j.1471-1842.2009.00848.x

Greenleaf, G. (2017). Global data privacy laws 2017: 120 national data privacy laws, including Indonesia and Turkey. *Privacy Laws & Business International Report*, *45*, 10–13.

Hair, J. F., Anderson, R. E., Babin, B. J., & Black, W. C. (2010). *Multivariate Data Analysis: A Global Perspective.* (7th ed.). New Jersey: Pearson Education.

Herath, K. M. (2011). *Building a Privacy Program. A Practitioner's Guide.* (2nd ed.). Portsmouth: International Association of Privacy Professionals (IAPP).

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems*, *18*(2), 106–125. http://doi.org/10.1057/ejis.2009.6

Herold, R. (2005). Building an effective privacy program. *EDPACS*, *33*(3), 9–24.

Heyink, M. (2011). Protection of personal information guidelines for law firms. *Law Society of South Africa*, 1-22. Retrieved April 24, 2019 from https://www.lssa.org.za/upload/files/Resource%20documents/Protection%20of%20Personal%20Information%20for%20South%20African%20Law%20Firms%20LSSA%20Guidelines%202018.pdf

Hinde, C. (2014). *A Model to Assess Organisational Information Privacy Maturity against the Protection of Personal Information Act*. (Master's dissertation). University of Cape Town, Cape Town.

Hughes, T., & Leizerov, S. (2016). IAPP-EY Annual Privacy Governance Report 2016. Retrieved January 29, 2019, from https://iapp.org/media/pdf/resource_center/IAPP-2016-GOVERNANCE-SURVEY-FINAL2.pdf

Hughes, T., & Saverice-Rohan, A. (2018). IAPP-EY Annual Privacy Governance Report 2018. Retrieved December 28, 2018, from https://iapp.org/media/pdf/resource_center/IAPP-EY-Gov_Report_2018-FINAL.pdf

Hui, K. L., Teo, H. H., & Lee, S. Y. T. (2007). The value of privacy assurance: An exploratory field experiment. *MIS Quarterly*, *31*(1), 19–33. http://doi.org/ 10.2307/25148779

Information Regulator (South Africa). (2016). Information Regulator in South Africa. Retrieved January 29, 2019, from http://www.justice.gov.za/inforeg/index.html

Information Regulator South Africa. (2017). Information Regulator of South africa 2017-2020 Strategic Plan. Retrieved January 29, 2019, from http://www.justice.gov.za/inforeg/docs/InfoRegSA-2017-2020StrategicPlan.pdf

Innes, J. C. (1992). *Privacy, Intimacy, and Isolation*. New York: Oxford University Press.

ISO/EIC. (2011). ISO/EIC 29100:2011 Information Technology: Security Techniques: Privacy Framework. Retrieved January 29, 2019, from https://www.iso.org/obp/ui/#iso:std:iso-iec:29100:ed-1:v1:en:biblref:3

Jordaan, Y., & Jordaan, A. C. (2004). Communicating the protection of information privacy. *Communicare: Journal for Communication Sciences in Southern Africa*, *23*(1), 137–148.

Kaiser, H. F. (1960). The application of electronic computers to factor analysis. *Educational and Psychological Measurement*, *20*(1), 141–151.

Kemp, R., & Moore, A. D. (2007). Privacy. *Library Hi Tech*, *25*(1), 58–78. http://doi.org/10.1108/07378830710735867

Kicheva, T. (2017). Management of employees from different generations - Challenge for Bulgarian managers and HR professionals, *Economic Alternatives* (1), 103–121.

King III Report. (2009). King Code of Governance for South Africa 2009. Retrieved January 29, 2019, from http://www.ngopulse.org/sites/default/files/king_code_of_governance_for_sa_2009_updated_june_2012.pdf

King IV Report. (2016). King IV Report on Corporate Governance for South Africa 2016. Retrieved January 29, 2019, from http://c.ymcdn.com/sites/ www.iodsa.co.za/resource/resmgr/king_iv/King_IV_Report/IoDSA_King_IV_Report_-_WebVe.pdf

Klievink, B., Bharosa, N., & Tan, Y. H. (2016). The collaborative realization of public values and business goals: Governance and infrastructure of public-private information platforms. *Government Information Quarterly*, *33*(1), 67–79. http://doi.org/10.1016/j.giq.2015.12.002

Kline, P. (1994). A general description of factor analysis. In *An Easy Guide to Factor Analysis* (1st ed., pp. 1–13). London: Routledge.

Krejcie, R. V, & Morgan, D. W. (1970). Determining sample size for research activities. *Educational and Psychological Measurement*, *30*, 607–610.

Kroener, I., & Wright, D. (2014). A strategy for operationalizing privacy by design. *The Information Society*, *30*(5), 355–365. http://doi.org/10.1080/01972243. 2014. 944730

Lowry, P. B., Moody, G., Vance, A., Jensen, M., Jenkins, J., & Wells, T. (2012). Using an elaboration likelihood approach to better understand the persuasiveness of website privacy assurances cues for online consumers. *Journal of the American Society for Information Science and Technology*, *53*(4), 755–776. http://doi.org/10.1002/asi

Martins, N., & Da Veiga, A. (2015). Factorial invariance of an information security culture assessment instrument for multinational organisations with operations. *Journal of Governance and Regulation*, *4*(4), 1–13.

Mattick, R., & Clarke, C. (1998). Development and validation of measure of social phobia scrutiny fear and social interaction anxiety. *Behavior Research and Therapy*, *36*(455), 70. http://doi.org/10.1016/S0005-7967(97)10031-6

Maxwell. (2004). Conceptual framework. *Journal of Educational Administration*, *30*(4), 33–64. http://doi.org/10.1186/1472-6963-11-23

Maxwell, J. A. (2012). Designing a qualitative study. In *Qualitative Research Design: An Interactive Approach* (Vol. 17, pp. 214–253). http://doi.org/10.1007/s10461-014-0839-3.HIV

McCallister, E., Grance, T., & Scarfone, K. (2010). Guide to protecting the confidentiality of personally identifiable information (PII). *NIST Special Publication 800-122 Guide*, (April 2010), 1–59. http://doi.org/10.6028/NIST.SP.800-122

McCowan, R. J. R., & McCowan, S. S. C. (1999). Item analysis for criterion-referenced tests. *Center for Development of Human Services*, 1–39. Retrieved January 29, 2019, from http://eric.ed.gov/ERICWebPortal/recordDetail?accno=ED501716

Michalsons. (2017). Protection of Personal Information Act Summary | POPIA. Retrieved January 29, 2019, from https://www.michalsons.com/focus-areas/privacy-and-data-protection/protection-of-personal-information-act-popia

Miles, M. B., & Huberman, A. M. (1994). Focusing and bounding the collection of data: The substantive start. In *Qualitative Data Analysis: An Expanded Sourcebook* (2nd ed., pp. 16–38). London: Sage Publication.

Miltgen, C. L., & Smith, H. J. (2015). Exploring information privacy regulation, risks, trust, and behavior. *Information & Management*, *52*(6), 741–759. http://doi.org/10.1016/j.im.2015.06.006

Moore, A. (2008). Defining privacy. *Journal of Social Philosophy*, *39*(3), 411–428. http://doi.org/10.1111/j.1467-9833.2008.00433.x

Moss, M. J. (2014). Generational Sub-cultures. (Master's dissertation). University of South Africa, Pretoria.

Muijs, D. (2004). *Doing Quantitative Research in Education with SPSS*. *The SAGE Dictionary of Social Research Methods.* (1st ed.). London: Sage Publication. http://doi.org/10.4135/9780857020116.n166

Nassaji, H. (2015). Qualitative and descriptive research : Data type versus data analysis. *Language Teaching Research*, *19*(2), 129–132. http://doi.org/10.1177/

1362168815572747

National Computing Centre. (2005). IT Governance: Developing a Successful Governance Strategy - A Best Practice Guide for Decision Makers in IT. Retrieved January 29, 2019, from https://www.isaca.org/Certification/CGEIT-Certified-in-the-Governance-of-Enterprise-IT/Prepare-for-the-Exam/Study-Materials/Documents/Developing-a-Successful-Governance-Strategy.pdf

Neuman, W. L. (2014). *Social Research Methods: Qualitative and Quantitative Approaches*. *Relevance of Social Research.* (7th ed., Vol. 8). England: Pearson Education Limited. http://doi.org/10.2307/3211488

Nielsen, J., & Landauer, T. K. (1993). Model of the finding of usability problems. *In Proceedings of the INTERACT'93 and CHI'93 Conference on Human Factors in Computing Systems (pp. 206-213). ACM.* http://doi.org/10.1145/169059.169166

Oates, B. J. (2006). *Researching Information Systems and Computing*. London: Sage Publication.

OECD. (2013). The OECD Privacy Framework. Retrieved January 25, 2019, from http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

Office of Privacy Commissioner. (2016). Getting Accountability Right with a Privacy Management Program. Retrieved October 10, 2016, from https://www.oipc.bc.ca/guidance-documents/1435

Office of the Australian Information Commissioner. (2015a). Guide to Securing Personal Information. Retrieved January 29, 2019, from https://www.oaic.gov.au/resources/agencies-and-organisations/guides/guide-to-securing-personal-information.pdf

Office of the Australian Information Commissioner. (2015b). Privacy Management Framework: Enabling Compliance and Encouraging Good Practice. Retrieved January 29, 2019, from https://www.oaic.gov.au/agencies-and-organisations/guides/privacy-management-framework

Osborne, J. W. (2015). What is rotating in exploratory factor analysis? *Practical Assessment, Research & Evaluation*, *20*(2), 1–7. http://doi.org/10.1037/ e55895 2014-001

Ouma, S. (2013). *M-health User Experience Framework for the Public Healthcare Sector.* (Doctoral thesis). Nelson Mandela Metropolitan University, Port Elizabeth.

Oxford Online Dictionary. (2017). Definition of Framework and Governance in English. Retrieved January 29, 2019, from https://0-premium.oxforddictionaries.com.oasis.unisa.ac.za/definition/english/framework

PAIA. (2000). Promotion of Access To Information Act 2 of 2000. Retrieved January 29, 2019, from http://www.justice.gov.za/legislation/acts/2000-002.pdf

Park, S. (2007). *Strategies and Policies in Digital Convergence*. Hershey and London: Idea Group Inc Publishing.

PCPD. (2014). Privacy Management Programme: A Best Practice Guide. Retrieved January 29, 2019, from https://www.pcpd.org.hk/pmp/files/PMP_guide_e.pdf

Pearson, S. (2012). Privacy management in global organisations. *IFIP International Federation for Information Processing*, 217–237.

Pearson, S. (2014). Privacy management and accountability in global organisations. *IFIP International Federation for Information Processing*, 33–52.

Pearson, S., Rao, P., Sander, T., Parry, A., Paull, A., Patruni, S., Dandamudi-Ratnakar, V., & Sharma, P. (2009). Scalable, accountable privacy management for large organizations. *13th Enterprise Distributed Object Computing Conference Workshops, 2009*, 168–175. http://doi.org/10.1109/EDOCW.2009.5331996

Pelkola, D. (2012). A framework for managing privacy-enhancing technology. *IEEE Software*, *29*(3), 45–49. http://doi.org/10.1109/MS.2012.47

Pilgrim, T. (2014). Privacy Governance Framework. Retrieved January 29, 2019, from https://www.ipc.nsw.gov.au/privacy-governance-framework

PIPEDA. (2015). Personal Information Protection and Electronic Documents Act 5 0f 2000. Retrieved January 29, 2019, from http://laws.justice.gc.ca/PDF/P-8.6.pdf

PricewaterhouseCoopers. (2017). Privacy Governance Survey: The State of Privacy Management in Belgian Organisations. Retrieved June 24, 2018, from https ://www.pwc.be/en/documents/20170313-privacy-governance-health-check.pdf

Raab, C. (2012). The Meaning of “Accountability” in the Information Privacy Context. In *Managing Privacy through Accountability* (pp. 15–32). Palgrave Macmillan.

Raizenberg, R. (2015). Towards Building a Privacy Programme: A Personal Journey. Retrieved January 29, 2019, from http://www.isaca.org/Knowledge-Center/Research/Documents/COBIT-Focus-towards-building-a-privacy-programme-a-personal-journey_nlt_Eng_1015.pdf

Rhodes, R. A. W. (1996). The new governance: Governing without government. *Political Studies*, *44*(4), 652–667. http://doi.org/10.1111/j.1467-9248.1996. tb 01747.x

Salaria, N. (2012). Meaning of the term descriptive survey. *International Journal of Transformations in Business Management*, *1*(6), 1–7.

Saunders, M., Lewis, P., & Thornhill, A. (2016). *Research Methods for Business Students*. *Business.* (7th ed.). England: Pearson Education Limited.

Schwartz, P. M., & Solove, D. J. (2011). The P11 problem: Privacy and a new concept of personally identifiable information. *New York University Law Review*, *86*, 1814–1894. http://doi.org/10.1525/sp.2007.54.1.23

Scott, K. L. (2015). Overview of the Privacy Act of 1974. Retrieved January 29, 2019, from https://www.justice.gov/opcl/introduction

Seerden, X., Salmela, H., & Rutkowski, A. (2018). Privacy governance and the GDPR :

How are organizations taking action to comply with the new privacy regulations in Europe ? *ECMLG 2018 14th European Conference on Management, Leadership and Governance*, *14*, 371–378.

Segal, S. (2015). New Privacy Management Framework to Help Business and Government Create Culture of Privacy. Retrieved January 29, 2019, from https://www.claytonutz.com/knowledge/2015/may/new-privacy-management-framework-to-help-business-and-government-create-culture-of-privacy

Shred-it. (2016). Lack of Awareness Putting South African Businesses at Risk of Data Breaches. Retrieved January 29, 2019, from https://www.shredit.co.za/getmedia/3c6d2d25-bc73-421f-a553-21d23a96871a/Shred-it_Security_Tracker_Infographic _South_Africa_2016.aspx?ext=.pdf

Sobh, R., & Perry, C. (2005). Research design and data analysis in realism research, *European Journal of marketing, 40*(11/12), 1194–1209. http://doi.org/10.1108/03090560610702777

Solomon, J. (2007). *Corporate Governance and Accountability.* (2nd ed.). England: John Wiley & Sons.

Solove, D. J. (2002). Conceptualizing privacy. *California Law Review*, *90*(4), 1087–1155. http://doi.org/10.1145/1929609.1929610

Solove, D. J. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review*, *154*(3), 477–560. http://doi.org/10.1145/1929609.1929610

Solove, D. J., & Hartzog, W. (2014). The FTC and the new common law of privacy. *Columbia Law Review*, *114*(3), 583–676.

South Africa. Protection of Personal Information Act (POPIA) No 4 of 2013, 581 Government Gazette 1–148 (2013). Retrieved January 29, 2019, from http://www.gov.za/documents/download.php?f=204368%5Cnhttp://www.greengazette.co.za/notices/act-no-4-of-2013-protection-personal-information-act-2013_20131126-GGN-37067-00912

Sreejesh, S., Mohapatra, S., & Anusree, M. R. (2014). *Business Research Methods:*

An Applied Orientation. New York : Springer. http://doi.org/10.1007/978-3-319-00539-3

Srivastava, M. (2009). Good governance - concept, meaning and features: A detailed study. *Social Science Research Network*, December 2009, 1–23. http://doi.org/10.2139/ssrn.1528449

Steenkamp, G. (2011). The applicability of using COBIT as a framework to achieve compliance with the King III Report's requirements for good IT governance. *Southern African Journal of Accountability and Auditing Research*, *11*(1), 1–8.

Sukamolson, S. (2007). Fundamentals of quantitative research. *Language Institute Chulalongkorn University*, 1–20.

Swartz, P., & Da Veiga, A. (2016). PoPI Act - opt-in and opt-out compliance from a data value chain perspective : A South African insurance industry experiment. *Information Security for South Africa (ISSA)*, 9–17. http://doi.org/10.1109/ISSA.2016.7802923

Tancock, D., Pearson, S., & Charlesworth, A. (2013). *A Privacy Impact Assessment Tool for Cloud Computing*. *Privacy and Security for Cloud Computing*. http://doi.org/10.1007/978-1-4471-4189-1

Teltzrow, M., & Kobsa, A. (2004). Impacts of User Privacy Preferences on Personalized Systems. Designing personalized user expereince in eCommerce, 315–332. Springer, Dordrecht

The Free Dictionary Online. (2017). Definition of Framework. Retrieved January 29, 2019, from http://www.thefreedictionary.com/framework

Thomas, G. (2006). The DGI Data Governance Framework. Retrieved January 29, 2019, from http://www.datagovernance.com/wp-content/uploads/2014/11/dgi_framework.pdf

Tjhin, I., Vos, M., & Munaganuri, S. (2016). Privacy governance online: Privacy policy on New Zealand websites. *Pacific Asia Conference on Information Systems (PACIS)*, 1–16.

Treiblmaier, H., & Filzmoser, P. (2010). Exploratory factor analysis revisited: How

robust methods support the detection of hidden multivariate data structures in IS research. *Information and Management*, *47*(4), 197–207. http://doi.org/10.1016/j.im.2010.02.002

United Nations. (1948). Universal Declaration of Human Rights. Retrieved January 2, 2019, from http://www.un.org/en/universal-declaration-human-rights/

Vael, M. (2017). Privacy Compliance Laws : Why the European Commission Has Finally Got It Right. Retrieved January 29, 2019, from https://www.csoonline.com/article/2132708/privacy/privacy-compliance-laws--why-the-european-commission-has-finally-got-it-right.html

Van Breugel, G., Van Olffen, W., & Olie, R. (2005). Temporary liaisons: The commitment of 'temps' towards their agencies. *Journal of Management Studies*, 42(3), 539–566.

Van den Honert, R. (1999). *Intermediate Statistical Methods for Business and Economics.* (2nd ed.). Cape Town: University of CapeTown Press.

Varkevisser, C. M., Pathmathan, I., & Brownlee, A. (2003). *Designing and Conducting Health Systems Research Projects.* (1st ed.). Amsterdam: KIT Publishers.

Weber, R. H. (2014). Privacy management practices in the proposed EU regulation. *International Data Privacy Law*, *4*(4), 290–297.

Weber, R. H. (2015). The digital future - A challenge for privacy? *Computer Law and Security Review*, *31*, 234–242. http://doi.org/10.1016/j.clsr.2015.01.003

Weiss, N. A. (2012). *Introductory Statistics.* (9th ed.). Boston: Pearson.

Wolters, K., Koorn, R., & Koetsier, M. (2016). EU General Data Protection Regulation Ratified. Retrieved January 29, 2019, from https://assets.kpmg.com/content/dam/kpmg/pdf/2016/05/EU-General-Data-Protection-Regulation-ratified-18-04-2016.pdf

Yin, R. K. (2009). *Case Study Research: Design and Methods*. *Sage Publications* (4th ed.). California: Sage Publication.

APPENDICES

Appendix A: Research permission letter

UNISA university of south africa

RESEARCH PERMISSION LETTER

Request for permission to conduct research at *Financial institution*

A privacy governance framework and questionnaire to measure the perception of effective privacy governance

15 March 2018

Company Address

Dear Mr.

I, Paulus Swartz am doing research with Dr. A. Da Veiga, senior lecturer in the Department of Computing and Prof N. Martins, research professor in the Department of Industrial and Organisational Psychology, towards an MSc in Computing at the University of South Africa. We are inviting you to participate in a study entitled "A privacy governance framework and questionnaire to measure the perception of effective privacy governance".

I would like to ask your permission to allow me to conduct a survey among the staff in the Infrastructure Service department. It is envisaged to receive a minimum of 400 responses from the staff.

The aim of this research is to develop a comprehensive privacy governance framework and also to develop an Information Privacy Governance Questionnaire to assess the perception of employees of how effective the organisation governs privacy.

Your organisation have been selected because of the different business units that process personal information of the clients by staff members.

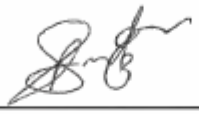
The study will entail the development of a conceptual privacy governance framework, which aid organization's to govern privacy, in line with POPIA and organisation policies. The overall outcome of the study will be a valid and reliable information privacy governance questionnaire to measure the perception of the employee's view of how effective privacy is governed within the organisation.

University of South Africa
Preller Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za

Participation in the survey is entirely voluntary and there is no unknown or anticipated risks to the participation in this study. The survey would last only about 15 minutes and would be arranged at a time convenient for the employees. All information provided will be kept in utmost confidentiality and would be used only for academic purposes. The name of the organisation will not appear in any dissertation or publication resulting from this study unless agreed to.

After the data have been analyzed, you will receive a copy of the executive summary. If you would be interested in greater detail, an electronic copy of the entire dissertation can be made available.

Yours sincerely



_____ (Researcher Signature)

Mr. Paulus Swartz

Student – 36278580

_____ (Approver Signature)

Manager: IT Operations

University of South Africa
Preller Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za

Appendix B: Ethical clearance certificate

UNISA university of south africa

UNISA COLLEGE OF SCIENCE, ENGINEERING AND TECHNOLOGY'S (CSET) RESEARCH AND ETHICS COMMITTEE

16 March 2018

Ref #: 005/PS/2018/CSET_SOC
Name: Mr Paulus Swartz
Student #: 36278580

RECEIVED
2018 -03- 19
OFFICE OF THE EXECUTIVE DEAN
College of Science, Engineering and Technology

Dear Mr Paulus Swartz

Decision: Ethics Approval for 3 years (Humans involved)

Researchers: Mr Paulus Swartz,
9 Thomas Street, Davidsonville, Roodepoort, 1724
36278580@mylife.unisa.ac.za, +27 11 760 4995, +27 71 480 9671

Project Leader(s): Dr A Da Veiga, dveiga@unisa.ac.za, +27 11 670 9175
Prof N Martins, martinsn@mweb.co.za, +27 12 429 8379

Proposal: A privacy governance framework and questionnaire to measures the perception of effective privacy governance

Qualification: MSc in Computing

Thank you for the application for research ethics clearance by the Unisa College of Science, Engineering and Technology's (CSET) Research and Ethics Committee for the above mentioned research. Ethics approval is granted for a period of three years, from 16 March 2018 to 16 March 2021.

1. The researcher will ensure that the research project adheres to the values and principles expressed in the UNISA Policy on Research Ethics.
2. Any adverse circumstance arising in the undertaking of the research project that is relevant to the ethicality of the study, as well as changes in the methodology, should be communicated in writing to the Unisa College of Science, Engineering and Technology's (CSET) Research and Ethics Committee. An amended application could

University of South Africa
Preller Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za

be requested if there are substantial changes from the existing proposal, especially if those changes affect any of the study-related risks for the research participants.

3. The researcher will ensure that the research project adheres to any applicable national legislation, professional codes of conduct, institutional guidelines and scientific standards relevant to the specific field of study.
4. Only de-identified research data may be used for secondary research purposes in future on condition that the research objectives are similar to those of the original research. Secondary use of identifiable human research data requires additional ethics clearance.
5. Permission to contact this research should be obtained from the financial institution prior to commencing field work.

Note:

The reference number 005/PS/2018/CSET_SOC should be clearly indicated on all forms of communication with the intended research participants, as well as with the Unisa College of Science, Engineering and Technology's (CSET) Research and Ethics Committee.

Yours sincerely

Dr. B Chimbo

Chair: Ethics Sub-Committee School of Computing, CSET

Prof I. Osunmakinde

Director: School of Computing, CSET

Prof B. Mamba

Executive Dean: College of Science, Engineering and Technology (CSET)

University of South Africa
Preller Street, Muckleneuk Ridge, City of Tshwane
PO Box 392, UNISA 0003 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za

Appendix C: Participant information sheet

PARTICIPANT INFORMATION SHEET

Ethics clearance reference number: 005/PS/2018/CSET_SOC

23 March 2018

Title: A privacy governance framework and questionnaire to measure the perception of effective privacy governance

Dear Prospective Participant

My name is Paulus Swartz and I am conducting a research with Dr. A. da Veiga, senior lecturer in the Department of Computing, and Prof. N. Martins, research professor in the Department of Industrial and Organisational Psychology, towards an MSc in Computing at the University of South Africa. We are inviting you to participate in a study entitled “A privacy governance framework and questionnaire to measure the perception of effective privacy governance”.

WHAT IS THE PURPOSE OF THE STUDY?

This study is expected to collect important information that could assist us to develop a comprehensive privacy governance framework and also to develop an IPGQ to assess the perception of employees of how effective the organisation governs privacy.

WHY AM I BEING INVITED TO PARTICIPATE?

Two groups will participate in the evaluation of the questionnaire. The first group is an expert panel and the second will conduct the pilot survey. For the expert panel group we envisage 5-10 people to participate. I have invited the expert panel members to participate in this study because of their expertise in the field of privacy and the protection of personal information.

Employees in the participating organisation will take part in the pilot study and are invited based on their interaction and use of systems in the organisations whereby personal information is processed. A group of about 10-20 people will participate in the pilot study.

WHAT IS THE NATURE OF MY PARTICIPATION IN THIS STUDY?

The study involves a survey whereby the participant must complete a questionnaire. Biographical, general awareness and privacy perception type of questions will be asked.

The expected review time for the expert panel is 1-2 weeks. During this time the expert panel will be given an opportunity to review the questionnaire and give input. The expected timeframe for the pilot group to complete the questionnaire is 10-15 minutes.

CAN I WITHDRAW FROM THIS STUDY EVEN AFTER HAVING AGREED TO PARTICIPATE?

Participating in this study is voluntary and you are under no obligation to consent to participation. If you do decide to take part, you will be given this information sheet to keep and be asked to sign a written consent form. You are free to withdraw at any time and without giving a reason. The survey is developed to be anonymous, meaning that we will have no way of connecting the information that you provide to you personally. Consequently, you will not be able to withdraw from the study once you have clicked the ‘send’ button based on the anonymous nature of the survey.

WHAT ARE THE POTENTIAL BENEFITS OF TAKING PART IN THIS STUDY?

You will not benefit from your participation as an individual; however, it is envisioned that the findings of this study will improve the protection of personal information in the participating organisation from a research perspective. It is anticipated that the information we gain from this survey will help us to develop a comprehensive privacy governance framework, and also to develop an Information Privacy Governance

Questionnaire to assess the perception of employees of how effective the organisation governs privacy.

ARE THERE ANY NEGATIVE CONSEQUENCES FOR ME IF I PARTICIPATE IN THE RESEARCH PROJECT?

We do not foresee that you will experience any negative consequences by completing the survey. The survey is anonymous and no personal identifiable information will be collected.

WILL THE INFORMATION THAT I CONVEY TO THE RESEARCHER AND MY IDENTITY BE KEPT CONFIDENTIAL?

Your name will not be recorded anywhere and no-one will be able to connect you to the answers /input you give. Your answers will be given a code number or a pseudonym and we will refer to you in this way in the data, any publications or other research reporting methods such as conference proceedings.

By completing this survey, the anonymous information you provide may be used for research purposes, including dissemination through peer-reviewed publications and conference proceedings. A report on the study may be submitted for publication but individual participants will not be identifiable in such report.

HOW WILL THE RESEARCHER(S) PROTECT THE SECURITY OF DATA?

Hard copies of your answers will be stored by the researcher for a minimum period of five years in a locked cupboard/filing cabinet at Unisa for future research or academic purposes; electronic information will be stored on a password-protected computer. Future use of the stored data will be subject to further research ethics review and approval, if applicable. Hard copies will be shredded, and data will be deleted permanently from the survey application database files and hard drive of the computer through the use of a relevant software application.

WILL I RECEIVE PAYMENT OR ANY INCENTIVES FOR PARTICIPATING IN THIS STUDY?

You will not benefit from your participation as an individual; however, it is envisioned that the findings of this study will improve the protection of personal information in ABC from a research perspective. You will not be reimbursed or receive any incentives for your participation in the survey.

HAS THE STUDY RECEIVED ETHICS APPROVAL?

This study has received written approval from the Research Ethics Review Committee of the School of Computing, Unisa. A copy of the approval letter can be obtained from the researcher if you so wish.

HOW WILL I BE INFORMED OF THE FINDINGS/RESULTS OF THE RESEARCH?

If you would like to be informed of the final research findings, please contact Paulus Swartz on +27(0) 11 550 2126 or email: 362758580@mylife.unisa.ac.za. The findings are accessible for a period of five years. Should you require any further information or want to contact the researcher about any aspect of this study, please contact Paulus Swartz on +27(0)115502126 or email: 362758580@mylife.unisa.ac.za.

Should you have concerns about the way in which the research has been conducted, you may contact Dr A. da Veiga on 011 670 9175 or email: dveiga@unisa.ac.za. Contact the research ethics chairperson of the School of Computing Research Ethics Committee on email: SocEthics@unisa.ac.za if you have any ethical concerns.

Thank you for taking time to read this information sheet and for participating in this study.

_____

P. Swartz

Appendix D: Participant consent form

UNISA university of south africa

CONSENT TO PARTICIPATE IN THIS STUDY

I, _____ (participant name), confirm that the person asking my consent to take part in this research has told me about the nature, procedure, potential benefits and anticipated inconvenience of participation.

I have read (or had explained to me) and understood the study as explained in the information sheet.

I have had sufficient opportunity to ask questions and am prepared to participate in the study.

I understand that my participation is voluntary and that I am free to withdraw at any time without penalty (if applicable).

I am aware that the findings of this study will be processed into a research report, journal publications and/or conference proceedings, but that my participation will be kept confidential unless otherwise specified.

I agree to the recording of the <insert specific data collection method>.

I have received a signed copy of the informed consent agreement.

Participant Name & Surname …… (Please print)

Participant Signature …… Date……

Researcher's Name & Surname …… (Please print)

Researcher's Signature …… Date……

University of South Africa
Preller Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za

Appendix E: Expert panel questionnaire

Ethical clearance: 005/PS/2018/CSET_SOC

PRIVACY PERCEPTION QUESTIONNAIRE
For expert panel

Dear expert panel member

You are invited to participate in a survey conducted by Paulus Swartz under the supervision of Dr A. da Veiga, a senior lecturer in the Department of Computing, and Prof. N. Martins, a research professor of Industrial and Organisational Psychology, towards an MSc in Computing degree at the University of South Africa.

The survey you have received has been designed to study the perceptions of employees in terms of how effective the organisation governs privacy. By completing this survey, you agree that the information you provide may be used for research purposes, including dissemination through peer-reviewed publications and conference proceedings.

It is anticipated that the information we gain from this survey will help us to develop a comprehensive privacy governance framework, and also to develop an Information Privacy Governance Questionnaire to assess the perception of employees of how effective the organisation governs privacy. You are, however, under no obligation to complete the survey and you can withdraw from the study prior to submitting the survey. The survey is developed to be anonymous, meaning that we will have no way of connecting the information that you provide to you personally. Consequently, you will not be able to withdraw from the study once you have clicked the ‘send’ button based on the anonymous nature of the survey. If you choose to participate in this survey it will take up no more than 15 minutes of your time. You will not benefit from your participation as an individual; however, it is envisioned that the findings of this study will improve the protection of personal information in ABC from a research perspective. We do not foresee that you will experience any negative consequences by completing the survey. The researcher(s) undertake to keep any information provided herein confidential, not to let it out of our possession and to report on the findings from the perspective of the participating group and not from the perspective of an individual.

The records will be kept for five years for audit purposes where after it will be destroyed permanently, and electronic versions will be deleted permanently from the hard drive of the computer. You will not be reimbursed or receive any incentives for your participation in the survey.

The research has been reviewed and approved by the School of Computing Research Ethics Committee 005/PS/2018/CSET_SOC. The primary researcher, Paulus Swartz, can be contacted during office hours at 011 550 2126. The study leader, Dr A. da Veiga, can be contacted during office hours at 011 670 9175. Should you have any questions regarding the ethical aspects of the study, you can contact the chairperson of the School of Computing Research Ethics Committee at SocEthics@unisa.ac.za Alternatively, you can report any serious unethical behaviour at the University's toll-free hotline 0800 86 96 93.

You are making a decision whether or not to participate by continuing to the next page. You are free to withdraw from the study at any time prior to clicking the 'send' button.

Information and definition section

It is fully acknowledged that you receive many requests to participate in surveys as a professional in your field. Therefore, your participation in this very important survey is sincerely appreciated.
The questionnaire consists of three sections, namely Section 1 where information about the expert panel is requested; Section 2 with six background questions, and Section 3 with the 66 privacy governance perception questions. We require the expert panel to indicate for each question whether they believe the item is essential to include or not, and whether it is clear or not.

Below are some definitions.

- **"Protection of Personal Information Act (POPIA) 4, 2013"**: This Act was signed into law in 2013 and promulgated to protect the privacy of individuals when personal information is processed by companies and public entities.
- **"Personal Information"**: Information that belongs or relate to a living, natural person that is identifiable; for example, gender, marital status, biometric information, birth of person, ethnic, health and well-being.

The questionnaire comprises 14 elements.

i. Leadership Commitment

The first condition of the POPIA is accountability which the organisation, as the responsible party, must act upon when processing personal information. To be accountable, the leadership (senior management) must be committed to ensure that the organisation is compliant with privacy legislation.

ii. Information Officer

Part B of Chapter 5 (Section 55) of the POPIA describes the responsibilities of an Information Officer and Deputy Information Officer. The role of the Information Officer is very important for the strategic planning of the business as well as the assessment and revision of the privacy programme.

iii. Privacy Office

The Privacy Office team usually consists of different team members from all areas of the organisation. The main responsibilities of the Privacy Office, identified by the IAPP-EY privacy governance survey, is the development of privacy policies and procedures; privacy awareness and training, privacy breach and incident management, the design and implementation of privacy controls, communication and privacy-impact assessment.

iv. Reporting

Principle 5 of the King IV Report states that the reports issued by the governing body of the organisation help the stakeholders to make informed assessments, and it also demonstrate that the organisation complies with the relevant laws.

v. Privacy Policies and Procedures

Policies and operational plans are developed by management that give direction in regard to privacy strategies according to the King IV Report and must be approved by the governing body.

vi. Personal Information Inventory

The organisation, therefore, has to keep an inventory of the personal information records they process. Organisations must document and understand the personal information they process and where it is stored.

vii. Breach Handling / Incident Management

Privacy breaches and security incidents can occur due to unauthorised access to data, negligence of employees and/or malicious and criminal attacks. Breach-handling procedures must be documented clearly and include five activities, namely detection, escalation, breach handling, breach notification and reporting.

viii. Service Provider Management

Third-party agreements and audit procedures must be in place to ensure compliance with the organisation's privacy policies and procedures. The service provider must comply with the service-level agreement or contract which includes adherence to the organisation's privacy policies and procedures.

ix. Communication

Condition 6 of the POPIA requires the responsible party to be open and transparent. Organisations have a responsibility to inform the individuals of their privacy rights by means of privacy notices on their websites and social media, and through mobile communication.

x. Privacy Awareness and Training

Privacy training must be conducted annually to assess the employees' understanding of any new changes to the privacy policies and procedures as well as to update employees on these changes.

xi. Risk Assessment Tools

Privacy-impact assessments can assist organisations in mitigating and identifying security risks and leakages. Risk assessment procedures must be in place to assess, identify and manage the privacy risk.

xii. Programme Assurance / Audit

This element ensure that internal and external audits are conducted to monitor compliance with the privacy policies. It improves the privacy processes while also being able to conduct internal audits

in order to identify areas of improvement. In addition, this element ensures that privacy self-assessments are conducted by the business units.

xiii. Oversight and Review Plan

An oversight and review plan must be implemented by the privacy officer to ensure that the privacy management programme is monitored and assessed effectively. The objective of the review plan ensures that the privacy operations are executed in alignment with the defined privacy processes.

xiv. Evaluate Privacy Practices

Privacy controls must be evaluated and updated on a regular basis. These controls are the policies and procedures; personal information inventory, privacy awareness and training, breach and incident management, communication and service provider management.

On the next page please find the questionnaire. Completion is expected to take no more than 15 minutes.

Section 1: Expert panel information

We require some background information about the experts involved in reviewing the questionnaire and would appreciate if you would complete the questions below.

i. What is your field of expertise (e.g. IT technician, legal, academic, privacy consultant)?
_____

ii. What is your current job title?
_____

iii. What experience do you have in information privacy governance?
_____

iv. How many years' experience do you have in information privacy?
_____

v. What experience do you have in the Protection of Personal Information Act?
_____

vi. How many years' experience do you have in services/work relating to the Protection of Personal Information Act?
_____

vii. What is your highest educational qualification?
_____

The survey is conducted to determine the perceptions of employees in terms of how effective the organisation governs privacy.

Instructions

Please provide one response to each item in the questionnaire, starting on the next page.

Indicate with a tick (✔) as to whether you believe the item is essential to include or not, and whether it is clear or not.

Section 2 – General awareness

Section 2 – General Awareness				Expert panel – select 1 answer here			
		Please indicate with a tick (✔)		Not essential	Essential	Item is clear	Item is unclear
		Yes	No				
1	I know who the Information Officer in ABC is.						
2	I have read the data privacy policies of ABC.						
3	I know where to get a copy of the data privacy policies.						
4	I received induction training covering privacy when I joined ABC.						
5	I received or attended privacy training in the last year.						
6	I know the contact details of the Privacy Office.						

Section 3– Privacy governance perception

Section 3 – Privacy Governance Perception							Expert panel - select 1 answer here			
		Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Not essential	Essential	Item is clear	Item is unclear
Leadership Commitment										
7	ABC is committed to the protection of personal information.									
8	The privacy policies are in line with the privacy strategy.									
9	Management provides me with adequate guidance to implement the regulatory requirements of the Protection of Personal Information Act in my daily duties.									
10	ABC has a function to effectively oversee the privacy programme.									

		Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Not essential	Essential	Item is clear	Item is unclear
Information Officer										
11	The Information Officer ensures compliance with the regulatory requirements of the Protection of Personal Information Act.									
12	The Information Officer's role is effective to give input to business decision-making in ABC.									
13	The Information Officer ensures that the privacy controls (e.g. training, audits, risk assessments, incident management) are implemented in ABC.									
14	The Information Officer effectively revises the privacy controls annually.									
15	The Information Officer effectively promotes a culture of privacy.									

		Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Not essential	Essential	Item is clear	Item is unclear
Privacy Office										
16	The Privacy Office effectively manages the protection of personal information in every major function.									
17	I am aware of the privacy controls in the application/s that I am using.									
18	I am aware of the privacy controls in the procedural functions that I have to follow.									
19	The resources of the Privacy Office are effective in promoting privacy awareness.									
20	I am aware of the role of the Privacy Office.									
21	My business unit has a clear reporting line to the Privacy Office.									

		Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Not essential	Essential	Item is clear	Item is unclear
Reporting										
22	My department receives privacy reports annually.									
23	The privacy reports are comprehensive enough to develop remediation plans.									
24	I am aware of the contents of the privacy compliance report.									
25	I believe I should receive the privacy report that affects my daily duties.									
26	I am aware of the escalation process in ABC to report any privacy issue.									
Privacy Policies and Procedures										
27	The privacy policy is understandable.									

		Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Not essential	Essential	Item is clear	Item is unclear
28	The privacy statement on the ABC website is understandable.									
29	The privacy policy assists me with the implementation of privacy controls in my daily duties.									
30	The privacy principles I follow in my daily duties are clearly defined in the privacy policies.									
31	The business processes and procedures are supported by the privacy policy.									
32	There are clear privacy standards and procedures in our business unit.									
Personal Information Inventory										
33	I know how to identify personal information.									
34	I know how to identify sensitive personal information.									

		Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Not essential	Essential	Item is clear	Item is unclear
35	Personal information collected by ABC is relevant for my daily tasks.									
36	Reasons for collecting and processing personal information are documented.									
Breach Handling / Incident Management										
37	The privacy procedures are effective to prevent a privacy breach or incident.									
38	I am aware of the incident management procedure in ABC to report a privacy incident.									
39	I am aware of the breach-handling procedure in ABC to report a privacy incident.									
40	I am aware of the consequences for the violation of privacy policies and procedures.									

		Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Not essential	Essential	Item is clear	Item is unclear
41	I am aware of the harmful effects (e.g. ABC brand and reputational damage, loss of market share and revenue, customer distrust and legal action against the company) of the violation of privacy policies and procedures.									
42	The breach-handling / incident management process of ABC is effective in resolving privacy incidents.									
Service Provider Management										
43	A third-party contract is in place between ABC and all service providers.									
44	Service providers adhere to the privacy requirements in the third-party contract of ABC.									
45	Audits are conducted effectively to ensure that the service providers are compliant with ABC's privacy requirements as stipulated in the third-party contract.									

		Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Not essential	Essential	Item is clear	Item is unclear
46	Data-privacy training for service providers is effective.									
Communication										
47	I have been informed about my privacy rights by ABC.									
48	ABC has communicated the purpose for collecting the personal information to the staff.									
49	I have read the privacy notice on ABC's website.									
50	ABC will notify me if my personal information has been compromised.									
51	My colleagues are aware of privacy changes that affect their daily duties.									

		Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Not essential	Essential	Item is clear	Item is unclear
52	I have a clear understanding of all privacy communications.									
Privacy Awareness and Training										
53	Newly appointed colleagues are provided with privacy training.									
54	Privacy training is customised for my job role.									
55	Privacy training has equipped my colleagues to implement the privacy policy.									
56	I have completed the mandatory privacy compliance test.									
57	The privacy compliance test covers changes to the privacy policies.									

		Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Not essential	Essential	Item is clear	Item is unclear
Risk Assessment Tools										
58	ABC's privacy risk assessments are performed regularly.									
59	New processes or systems are assessed for any potential privacy risk.									
60	Privacy risks of existing processes are reviewed.									
61	ABC's risk assessments help to identify privacy risks.									
Programme Assurance / Audit										
62	Privacy audits are conducted effectively to monitor compliance with privacy policies and procedures.									
63	Weaknesses or non-compliance with the privacy policies is revised.									

		Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Not essential	Essential	Item is clear	Item is unclear
64	Privacy self-assessments adequately prepares my department to be privacy compliant.									
65	The Privacy Office effectively prepares my division for privacy audits.									
Oversight and Review Plan										
66	Privacy is monitored effectively within my department.									
67	The recommendations of the privacy review plan are adequate.									
68	My business unit receives updates on the privacy review schedule.									
69	Privacy policies are reviewed for new technological advancements and systems.									

		Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Not essential	Essential	Item is clear	Item is unclear
Evaluate Privacy Practices										
70	Privacy controls (e.g. secure print, end-point protection, disk encryption, etc.) are evaluated.									
71	Privacy policies and procedures are updated regularly with technological changes.									
72	My business unit regularly receives privacy practice updates.									

Appendix F: Pilot group questionnaire

Ethical clearance: 005/PS/2018/CSET_SOC

PRIVACY PERCEPTION QUESTIONNAIRE
For pilot group

Dear pilot group member

You are invited to participate in a survey conducted by Paulus Swartz under the supervision of Dr A. da Veiga (senior lecturer in the School of Computing) and Prof. N. Martins (research professor of Industrial and Organisational Psychology) towards obtaining an MSc degree in Computing at the University of South Africa.

This survey has been designed to study the perceptions of employees in terms of how effective the organisation is at governing privacy. By completing this survey you agree that the information you provide may be used for research purposes as well as for dissemination through peer-reviewed publications and conference proceedings.

It is anticipated that the information we gain from this survey will help us to develop a comprehensive privacy governance framework and an Information Privacy Governance Questionnaire that will assess how effective employees perceive the organisation to be at governing privacy. You are, however, under no obligation to complete the survey and may withdraw from the study at any time prior to submitting it. The survey has been developed to be anonymous, meaning that we will have no way of connecting the information that you provide to you personally. Consequently, we will not be able to extract your information from the study once you have clicked the 'send' button. If you choose to participate in this survey, it will take no more than 15 minutes of your time. Although you as an individual will not benefit from your participation, it is envisioned that the findings of this study will improve the protection of personal information in your organisation from a research perspective. We do not foresee that you will experience any negative consequences by completing the survey. As researchers we undertake to keep any information provided herein confidential, not to let it go out of our possession, and to report on the findings from the perspective of the participating group (and not from that of an individual).

The records will be kept for five years for audit purposes, after which it will be permanently destroyed, and electronic versions will be deleted permanently from the hard drive of the computer. Furthermore, you will not be reimbursed or receive any incentives for your participation in the survey.

The research was reviewed and approved by the School of Computing Research Ethics Committee 005/PS/2018/CSET_SOC. The primary researcher, Paulus Swartz, can be contacted during office hours on 011 550 2126. The study leader, Dr A. da Veiga, is available during office hours on 011 670 9175. Should you have any questions regarding the ethical aspects of the study, you may

contact the chairperson of the School of Computing Research Ethics Committee at SocEthics@unisa.ac.za. Alternatively, you can report any serious unethical behaviour on the University's toll-free hotline 0800 86 96 93.

You now make your decision on whether to participate by continuing to the next page. **You are still free to withdraw from the study at any time prior to clicking the 'send' button**.

I consent to the above and wish to proceed with the survey.

Information and definition section

It is fully acknowledged that as a professional in your field you receive many requests to participate in surveys. Therefore, your participation in this very important survey is sincerely appreciated. The questionnaire consists of three sections: Section 1 where biographical information is requested, Section 2 with 8 background questions, and Section 3 with 68 questions on your privacy governance perception.

Definitions

- **"Protection of Personal Information Act (POPIA), 4 of 2013"**: This Act was signed into law in 2013 and promulgated to protect the privacy of individuals when their personal information is processed by companies and public entities.

- **"Personal information"**: Information that relates to an identifiable living, natural person; for example, gender, marital status, biometric information, birth date, ethnic origin, health and well-being as well as information that relates to an identifiable, existing juristic person.

- **"Personally identifiable information (PII)"**: Any information that (a) can be used to identify the PII principal to whom such information relates, or (b) is or might be directly or indirectly linked to a PII principal.

- **"Privacy culture"**: Environment or "culture" (integrated pattern of human knowledge, belief or behaviour, "the way things are done") that aims to protect a customer's privacy. It is a priority for every employee who handles personal information.

- **"Privacy controls"**: Measures that treat privacy risks by reducing their likelihood or their consequences.
    - Privacy controls include organisational, physical and technical measures, e.g. policies, procedures, guidelines, legal contracts, management practices or organisational structures.
    - Control is also used as a synonym for 'safeguard' or 'countermeasure'.

- **"Privacy incident"**: A privacy incident results from the loss of control, compromise, unauthorised disclosure, unauthorised acquisition, unauthorised access or any similar term referring to situations where persons other than authorised users, and for other than authorised purposes, have access or potential access to PII in usable form, whether physical or electronic. E.g. misdirected email – i.e. sending an email containing sensitive data (including high-risk and moderate-risk data) to an incorrect party.

- **“Privacy breach”**: Situations where personally identifiable information is processed in violation of one or more relevant privacy safeguarding requirement which triggers reporting obligations under the privacy law to those individuals whose information has been compromised.

- **“Privacy risk”**: Effect of uncertainty on privacy
    - Risk is defined as the “effect of uncertainty on objectives”.
    - Uncertainty is the state, or even partial state, of deficiency of information relating to the understanding or knowledge of an event, its consequence, or likelihood.

- **“Security safeguards”**: Personal information controllers should protect the personal information that they hold with appropriate safeguards against risks such as loss or unauthorised access to personal information or the unauthorised destruction, use, modification or disclosure of information, etc.

On the next page you will find the questionnaire. Completion is not expected to take more than 15 minutes.

We require some background information and would appreciate it if you would answer the questions below.

Instructions

Please provide one response to each item in the questionnaire. Indicate your selection with a tick (✔).

Section 1 – Biographical information											
1	Please indicate your age.	1925 - 1945	1946 - 1954	1955 - 1964	1965 - 1980	1981 - 2000					
2	Please indicate your gender.	Male				Female					
3	Please indicate your employment status.	Permanent		Contract		Vendor					
4	Please indicate your job level.	Administration	Operational	Team Leader	Line Manager	Senior Management	Executive				
5	Please indicate your length of service.	1-3 years		4-6 years		7-9 years		10+ years			
6	Please specify your business unit.	Retail / Business Banking	Insurance	IT	Investment Banking	HR	Legal	Operations	Marketing/ Communi-cation	Risk/ Compliance/ Auditing	Finance

Section 2 – General awareness

We require some privacy awareness information and would appreciate it if you would answer the questions below.

Instructions

Please provide one response to each item in the questionnaire.

Indicate your selection with a tick (✔).

Section 2 – General awareness			
		Please indicate with a tick (✔)	
		Yes	No
1	I know who the Information Officer in my organisation is.		
2	I have read the data privacy policies of my organisation.		
3	I know where to get a copy of the data privacy policies.		
4	I received induction training covering privacy when I joined my organisation.		
5	I received or attended privacy training in the last year.		
6	I know the contact details of the Privacy Office.		
7	I am aware that my organisation has a privacy notice on their website.		
8	I completed the mandatory privacy compliance test.		

Section 3 – Privacy governance perception

Section 3 – Privacy governance perception						
		Strongly disagree	Disagree	Neutral	Agree	Strongly agree
Leadership Commitment						
9	My organisation is committed to the protection of personal information.					
10	Management provides me with adequate guidance to implement the regulatory requirements of POPIA in my daily duties.					
11	I believe that my organisation effectively governs the protection of personal information with which we work.					
12	Management leads by example to protect personal information.					

		Strongly disagree	Disagree	Neutral	Agree	Strongly agree
Information Officer						
13	I believe that my organisation is effective in ensuring that the staff complies with POPIA requirements.					
14	We are encouraged to obtain input from the Information Officer for important business decisions.					
15	I believe that my organisation is effective in implementing the necessary privacy controls.					
16	I believe that my organisation continuously improves the privacy controls.					
17	My organisation has a strong privacy culture.					

		Strongly disagree	Disagree	Neutral	Agree	Strongly agree
Privacy Office						
18	My organisation ensures that personal information is protected in all our applications.					
19	My organisation effectively ensures that personal information is protected in all our processes.					
20	I have received clear communication from my organisation regarding privacy requirements (e.g. how to protect customer data).					
21	I am aware of the role of the Privacy Office.					
22	My organisation effectively informs us about privacy issues.					

		Strongly disagree	Disagree	Neutral	Agree	Strongly agree
Reporting						
23	My organisation clearly informs us about the responsibility and accountability roles for privacy.					
24	The reporting structures for privacy are clear in my organisation.					
25	I am aware of the timeframe to report a personal data compromise (privacy breach).					
26	All of us know what our responsibilities are for the protection of personal information.					
Privacy Policies and Procedures						
27	The privacy policy is understandable.					

		Strongly disagree	Disagree	Neutral	Agree	Strongly agree
28	The privacy statement on my organisation's website is understandable.					
29	The privacy policy guides me in the implementation of privacy processes in my daily duties.					
30	The privacy principles (e.g. accountability, openness, security safeguards and information quality) I follow in my daily duties are clearly defined in the privacy policies.					
31	I believe that the business processes and procedures are aligned with the privacy policy.					
32	There are clear privacy standards and procedures in my organisation (e.g. use, disclosure and safeguarding of personal information).					

		Strongly disagree	Disagree	Neutral	Agree	Strongly agree
Personal Information Inventory						
33	I know how to identify personal information.					
34	I know how to identify special (sensitive) personal information.					
35	My organisation only collects personal information for defined purposes.					
36	I am aware of the business need to collect and process personal information.					
Breach Handling / incident Management						
37	My organisation effectively deals with privacy breaches or incidents.					

		Strongly disagree	Disagree	Neutral	Agree	Strongly agree
38	I am aware of the incident management procedure in my organisation to report a privacy incident (e.g. misdirected email containing personal information).					
39	My organisation clearly communicates what procedure we must follow in the event of a data breach.					
40	I am aware of the consequences of the violation of privacy policies and procedures.					
41	I am aware of the escalation process in my organisation to report a privacy incident.					
42	I am aware of the timeframe to report a personal data compromise (privacy breach).					
43	I am aware of the harmful effects (e.g. on my organisation's brand and reputational damage, loss of market share and revenue, customer distrust or legal action against the company) of the violation of privacy policies and procedures.					

		Strongly disagree	Disagree	Neutral	Agree	Strongly agree
Service Provider Management						
44	I am confident that a contract is in place between my organisation and all service providers.					
45	Service providers are required to adhere to the privacy requirements in their contracts with my organisation.					
46	I am confident that my organisation ensures that service providers protect customers' personal information.					
47	I am confident that my organisation ensures that service providers (e.g. third parties, external consultants and contractors) receive training to protect customers' personal information.					

		Strongly disagree	Disagree	Neutral	Agree	Strongly agree
Communication						
48	My organisation informs me about my privacy rights.					
49	My organisation has communicated the purpose for collecting customers' personal information.					
50	My organisation will notify me if my personal information has been compromised.					
51	My organisation informs us when there are changes in processes to protect personal information.					
52	The communications that my organisation sends out about the protection of information are always understandable.					

		Strongly disagree	Disagree	Neutral	Agree	Strongly agree
Privacy Awareness and Training						
53	Newly appointed colleagues are provided with privacy training					
54	Privacy training is customised for my job role.					
55	The privacy training equips me to adhere to the privacy policy.					
56	My organisation expects me to complete an annual privacy compliance test.					
57	The privacy training helps me to understand how to protect personal information.					

		Strongly disagree	Disagree	Neutral	Agree	Strongly agree
Risk Assessment Tools						
58	I am confident that my organisation effectively implements measures to identify privacy risks.					
59	I am confident that new processes or systems are assessed for any potential privacy risk (e.g. new application, remote account opening and online applications).					
60	I believe that my organisation is effective in managing privacy risks.					
Programme Assurance / Audit						
61	I am confident that my organisation effectively conducts reviews (e.g. internal audits, external audits and self-assessment) to monitor compliance with its privacy policies and procedures.					

		Strongly disagree	Disagree	Neutral	Agree	Strongly agree
62	I am confident that my organisation effectively monitors compliance with its privacy policies and procedures.					
63	I am confident that my organisation improves the protection of personal information if a weakness is identified.					
64	I believe that the privacy self-assessments adequately prepare my department to be privacy compliant.					
65	I believe that the privacy office effectively prepares my division for privacy audits.					
Ongoing Assessment and Evaluation						
66	I am confident that my organisation ensures that its privacy policies are aligned with the latest technological advancements.					

		Strongly disagree	Disagree	Neutral	Agree	Strongly agree
67	I am confident that my organisation's privacy controls (e.g. secure print, end-point protection, disk encryption) are effective to protect personal information.					
68	My business unit regularly receives privacy practice updates.					

Appendix G: Final questionnaire – online version

Privacy Perception Questionnaire
June/July 2018

PRIVACY PERCEPTION QUESTIONNAIRE

June/July 2018

Scroll to the bottom of the screen and click on NEXT

Privacy Perception Questionnaire
June/July 2018

Ethical clearance #: 005/PS/2018/CSET_SOC

PRIVACY PERCEPTION QUESTIONNAIRE

Dear Prospective participant,

You are invited to participate in a survey conducted by Paulus Swartz under the supervision of Dr A. Da Veiga, a senior lecturer in the Department of Computing and Prof N. Martins, a research professor of Industrial and Organisational Psychology, towards an MSc in Computing degree at the University of South Africa.

The survey you have received has been designed to study the perceptions of employees in terms of how effective the organisation governs privacy. By completing this survey, you agree that the information you provide may be used for research purposes, including dissemination through peer-reviewed publications and conference proceedings.

It is anticipated that the information we gain from this survey will help us to develop a comprehensive privacy governance framework and also to develop an Information Privacy Governance Questionnaire to assess the perception of employees of how effective the organisation governs privacy. You are, however, under no obligation to complete the survey and you can withdraw from the study prior to submitting the survey. The survey is developed to be anonymous, meaning that we will have no way of connecting the information that you provide to you personally. Consequently, you will not be able to withdraw from the study once you have clicked the send button based on the anonymous nature of the survey. If you choose to participate in this survey it will take up no more than 15 minutes of your time. You will not benefit from your participation as an individual, however, it is envisioned that the findings of this study will improve the protection of personal information in the organisation from a research perspective. We do not foresee that you will experience any negative consequences by completing the survey. The researcher(s) undertake to keep any information provided herein confidential, not to let it out of our possession and to report on the findings from the perspective of the participating group and not from the perspective of an individual.

The records will be kept for five years for audit purposes where after it will be permanently destroyed and electronic versions will be permanently deleted from the hard drive of the computer. You will not be reimbursed or receive any incentives for your participation in the survey.

The research was reviewed and approved by the School of Computing Research Ethics Committee 005/PS/2018/CSET_SOC. The primary researcher, Paulus Swartz, can be contacted during office hours at 011 550 2126. The study leader, Dr A. Da Veiga, can be contacted during office hours at 011 670-9175. Should you have any questions regarding the ethical aspects of the study, you can contact the chairperson of the School of Computing Research Ethics Committee at SocEthics@unisa.ac.za. Alternatively, you can report any serious unethical behaviour at the University's Toll Free Hotline 0800 86 96 93.

You are making a decision whether or not to participate by continuing to the next page. You are free to withdraw from the study at any time prior to clicking the send button.

I consent to the above and to proceed with the survey:

Click on NEXT.

Information and definition section

It is fully acknowledged that as a professional in your field you receive many requests to participate in surveys. Therefore, your participation in this survey is sincerely appreciated.

The questionnaire consists of three sections: Section 1 where biographical information is requested, Section 2 with 8 background questions, and Section 3 with 68 questions on your privacy governance perceptions.

Definitions

> Protection of Personal Information Act (POPIA), 4, 2013: This Act was signed into law in 2013 and was promulgated to protect the privacy of individuals when their personal information is processed by companies and public entities.

> Personal Information: Information that relates to an identifiable living, natural person; for example gender, marital status, biometric information, birth date, ethnic origin, health and well-being, as well as information that relates to an identifiable, existing juristic person.

> Personally Identifiable Information (Pl I): Any information that (a) can be used to identify the Pl I Principal to whom such information relates, or (b) is or might be directly or indirectly linked to a Pl I principal.

> Privacy culture: Environment or "culture" (integrated pattern of human knowledge, belief or behaviour, "the way things are done") that aims to protect a customer's privacy. It is a priority for every employee who handles personal information.

> Privacy controls: Measures that treat privacy risks by reducing their likelihood or their consequences.

- Privacy controls include organisational, physical and technical measures, e.g. policies, procedures, guidelines, legal contracts, management practices or organisational structures.
- Control is also used as a synonym for safeguard or countermeasure.

Continues on next slide .....

Definitions continued ...

> Privacy incident: A privacy incident results from the loss of control, compromise, unauthorised disclosure, unauthorised acquisition, unauthorised access, or any similar term referring to situations where persons other that authorised users, and for other than authorised purposes, have access or potential access to Pl I in usable form, whether physical or electronic.
E.g. misdirected email - i.e., sending an email containing sensitive data (including high risk and moderate risk data) to an incorrect party.

> Privacy breach: Situation where personally identifiable information is processed in violation of one or more relevant privacy safeguarding requirements, which triggers reporting obligations under the privacy law to those individuals whose information was compromised.

> Privacy risk: Effect of uncertainty on privacy
- Risk is defined as the "effect of uncertainty on objectives"
- Uncertainty is the state, or even partial state, of deficiency of information relating to the understanding or knowledge of an event, its consequence, or likelihood.

> Security Safeguards: Personal information controllers should protect the personal information that they hold with appropriate safeguards against risks such as loss or unauthorised access to personal information, or the unauthorised destruction, use, modification or disclosure of information, etc.

On the next page you will find the questionnaire. Completion is not expected to take more than 15 minutes.

Please complete the survey in one session (cannot be book marked or saved and returned to later)

Thank you for your co-operation!

TECHNICAL DIFFICULTIES

For any **technical difficulties** please contact Ellen 083 457 9550 or send an e-mail to: orgdia@iafrica.com

Section 1: Biographical Information

We require some background information and would appreciate it if you would answer the questions below.

Instructions

Please provide one response to each item in the questionnaire.

Indicate your selection with a click in the circle.

Make sure a bullet appears in the circle that you select.

Section 1 - Biographical

1. **Please indicate your age**
   - ○ 1925 - 1945
   - ○ 1946 - 1954
   - ○ 1955 - 1964
   - ○ 1965 - 1980
   - ○ 1981 - 2000

2. **Please indicate your gender**
   - ○ Male
   - ○ Female
   - ○ Prefer not to disclose

3. **Please indicate your employment status**
   - ○ Permanent
   - ○ Contract
   - ○ Vendor

4. **Please indicate your job level**

- ○ Administration
- ○ Operational
- ○ Team Leader
- ○ Line Manager
- ○ Senior Management
- ○ Executive

5. **Please indicate your length of service**

- ○ 1 - 3 years
- ○ 4 - 6 years
- ○ 7 - 9 years
- ○ 10 years and more

6. **Please specify your business unit**

- ○ Finance
- ○ HR
- ○ Insurance
- ○ Investment Banking
- ○ IT
- ○ Legal
- ○ Marketing or Communication
- ○ Operations
- ○ Retail or Business Banking
- ○ Risk or Compliance or Auditing

Section 2: General Awareness

We require some privacy awareness information and would appreciate it if you would answer the questions below.

Instructions

Please provide one response to each item in the questionnaire.

Please indicate with a tick in the circle.

Make sure a bullet appears in the circle that you select.

Section 2 - General Awareness

		Yes	No
7.	I know who the Information Officer in my organisation is.	○	○
8.	I have read the Data Privacy Policies of my organisation.	○	○
9.	I know where to get a copy of the Data Privacy Policies.	○	○
10.	I received induction training covering privacy when I joined my organisation.	○	○
11.	I received or attended privacy training in the last year.	○	○
12.	I know the contact details of the privacy office.	○	○
13.	I am aware that my organisation has a privacy notice on their website.	○	○
14.	I completed the mandatory privacy compliance test.	○	○

Section 3: Privacy Governance Perception

Leadership Commitment

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
15. My organisation is committed to the protection of personal information.	○	○	○	○	○
16. Management provides me with adequate guidance to implement the regulatory requirements of POPIA in my daily duties.	○	○	○	○	○
17. I believe that my organisation effectively governs the protection of personal information that we work with.	○	○	○	○	○
18. Management leads by example to protect personal information.	○	○	○	○	○

Information Officer

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
19. I believe that my organisation is effective in ensuring that the staff complies with POPIA requirements.	○	○	○	○	○
20. We are encouraged to obtain input from the Information Officer for important business decisions.	○	○	○	○	○
21. I believe that my organisation is effective in implementing the necessary privacy controls.	○	○	○	○	○
22. I believe that my organisation continuously improves the privacy controls.	○	○	○	○	○
23. My organisation has a strong privacy culture.	○	○	○	○	○

Privacy Office

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
24. My organisation ensures that personal information is protected in all our applications.	○	○	○	○	○
25. My organisation effectively ensures that personal information is protected in all our processes.	○	○	○	○	○
26. I have received clear communication from my organisation regarding privacy requirements (e.g. how to protect customer data).	○	○	○	○	○
27. I am aware of the role of the Privacy Office.	○	○	○	○	○
28. My organisation effectively informs us about privacy issues.	○	○	○	○	○

Reporting

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
29. My organisation clearly informs us about the responsibility and accountability roles for privacy.	○	○	○	○	○
30. The reporting structures for privacy are clear in my organisation.	○	○	○	○	○
31. I am aware of the time frame to report a personal data compromise (privacy breach).	○	○	○	○	○
32. All of us know what our responsibilities are for the protection of personal information.	○	○	○	○	○

Privacy Policies and Procedures

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
33. The privacy policy is understandable.	○	○	○	○	○
34. The privacy statement on my organisation's website is understandable.	○	○	○	○	○
35. The privacy policy guides me with the implementation of privacy processes in my daily duties.	○	○	○	○	○
36. The privacy principles (e.g. accountability, openness, security safeguards and information quality) I follow in my daily duties are clearly defined in the privacy policies.	○	○	○	○	○
37. I believe that the business processes and procedures are aligned with the privacy policy.	○	○	○	○	○
38. There are clear privacy standards and procedures in my organisation (e.g. use, disclosure and safeguarding of personal information).	○	○	○	○	○

Personal Information Inventory

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
39. I know how to identify personal information.	○	○	○	○	○
40. I know how to identify special (sensitive) personal information.	○	○	○	○	○
41. My organisation only collects personal information for defined purposes.	○	○	○	○	○
42. I am aware of the business need to collect and process personal information.	○	○	○	○	○

Breach Handling / Incident Management

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
43. My organisation effectively deals with privacy breaches or incidents.	○	○	○	○	○
44. I am aware of the incident management procedure in my organisation to report a privacy incident. (E.g. misdirected email containing personal information).	○	○	○	○	○
45. My organisation clearly communicates what procedure we must follow in the event of a data breach.	○	○	○	○	○
46. I am aware of the consequences of the violation of privacy policies and procedures.	○	○	○	○	○
47. I am aware of the escalation process in my organisation to report a privacy incident.	○	○	○	○	○
48. I am aware of the time frame to report a personal data compromise (privacy breach).	○	○	○	○	○
49. I am aware of the harmful effects (e.g. my organisation's brand and reputational damage, loss of market share and revenue, customer distrust or legal action against the company) of the violation of privacy policies and procedures.	○	○	○	○	○

Service Provider Management

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
50. I am confident that a contract is in place between my organisation and all service providers.	○	○	○	○	○
51. Service providers are required to adhere to the privacy requirements in their contracts with my organisation.	○	○	○	○	○
52. I am confident that my organisation ensures that service providers protect customers' personal information.	○	○	○	○	○
53. I am confident that my organisation ensures that service providers (e.g. third parties, external consultants and contractors) receive training to protect customers' personal information.	○	○	○	○	○

Communication

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
54. My organisation informs me about my privacy rights.	○	○	○	○	○
55. My organisation has communicated the purpose for collecting customers' personal information.	○	○	○	○	○
56. My organisation will notify me if my personal information has been compromised.	○	○	○	○	○
57. My organisation informs us when there are changes in processes to protect personal information.	○	○	○	○	○
58. The communications that my organisation send out about the protection of information are always understandable.	○	○	○	○	○

Privacy Awareness and Training

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
59. Newly appointed colleagues are provided with privacy training.	○	○	○	○	○
60. Privacy training is customised for my job role.	○	○	○	○	○
61. The privacy training equips me to adhere to the privacy policy.	○	○	○	○	○
62. My organisation expects me to complete an annual privacy compliance test.	○	○	○	○	○
63. The privacy training helps me to understand how to protect personal information.	○	○	○	○	○

Risk Assessment Tools

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
64. I am confident that my organisation effectively implements measures to identify privacy risks.	○	○	○	○	○
65. I am confident that new processes or systems are assessed for any potential privacy risk (e.g. new application, remote account opening, and online applications).	○	○	○	○	○
66. I believe that my organisation is effective in managing privacy risks.	○	○	○	○	○

Program Assurance/Audit

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
67. I am confident that my organisation effectively conducts review (e.g. internal audit, external audits, and self-assessment) to monitor compliance with its privacy policies and procedures.	○	○	○	○	○
68. I am confident that my organisation effectively monitors compliance with its privacy policies and procedures.	○	○	○	○	○
69. I am confident that my organisation improves the protection of personal information if a weakness is identified.	○	○	○	○	○
70. I believe that the privacy self-assessments adequately prepare my department to be privacy compliant.	○	○	○	○	○
71. I believe that the privacy office effectively prepares my division for privacy audits.	○	○	○	○	○

Ongoing Assessment and Evaluation

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
72. I am confident that my organisation ensures that its privacy policies are aligned with the latest technological advancements.	○	○	○	○	○
73. I am confident that my organisation's privacy controls (e.g. secure print, end-point protection, disk encryption) are effective to protect personal information.	○	○	○	○	○
74. My business unit regularly receives privacy practice updates.	○	○	○	○	○

Section 4: Open-ended Statement

75. Do you have any other comments or suggestions regarding the governing of privacy in the organisation? Please add your comments.

_____

_____

Thank you for your participation!

Scroll to the bottom of the screen and click on SUBMIT

NOTES ON SUBMISSION:

1. If you receive a '**thank you**' message after submitting, your submission has been successful.

2. If you are unable to submit, or receive any other message, please do not close the file, wait a short while and then try to submit again.

3. If the submit button fails, please save your answers to a .pdf format and email to orgdia@iafrica.com.

4. Contact details for technical difficulties: Ellen 083 457 9550 or send an e-mail to orgdia@iafrica.com.

Appendix H: One-way ANOVA statistics

One-way ANOVA – Employment Status group

		Sum of Squares	df	Mean Square	F	Sig.
Privacy controls assessment	Between Groups	2.006	1	2.006	4.210	0.041
	Within Groups	177.721	373	0.476		
	Total	179.727	374			
Personal information awareness assessment	Between Groups	1.206	1	1.206	2.913	0.089
	Within Groups	154.343	373	0.414		
	Total	155.549	374			
Privacy governance reporting	Between Groups	2.262	1	2.262	3.546	0.060
	Within Groups	237.884	373	0.638		
	Total	240.146	374			
Organisational commitment	Between Groups	2.843	1	2.843	5.695	0.018
	Within Groups	186.234	373	0.499		
	Total	189.077	374			

One-way ANOVA – Gender group

		Sum of Squares	df	Mean Square	F	Sig.
Privacy controls assessment	Between Groups	0.101	1	0.101	0.212	0.645
	Within Groups	178.032	373	0.477		
	Total	178.134	374			
Personal information awareness assessment	Between Groups	0.010	1	0.010	0.024	0.876
	Within Groups	146.468	373	0.393		
	Total	146.477	374			
Privacy governance reporting	Between Groups	0.008	1	0.008	0.012	0.912
	Within Groups	231.173	373	0.620		
	Total	231.180	374			
Organisational commitment	Between Groups	0.019	1	0.019	0.040	0.841
	Within Groups	178.537	373	0.479		
	Total	178.556	374			

Post Hoc Tests - Age group

Multiple Comparisons

Scheffé

Dependent Variable			Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
						Lower Bound	Upper Bound
Privacy controls assessment	1946-1964	1965-1980	0.04696	0.12283	0.930	-0.2549	0.3488
		1981-2000	-0.18169	0.11348	0.279	-0.4606	0.0972
	1965-1980	1946-1964	-0.04696	0.12283	0.930	-0.3488	0.2549
		1981-2000	-.22865*	0.08043	0.018	-0.4263	-0.0310
	1981-2000	1946-1964	0.18169	0.11348	0.279	-0.0972	0.4606
		1965-1980	.22865*	0.08043	0.018	0.0310	0.4263
Personal information awareness assessment	1946-1964	1965-1980	0.15757	0.11466	0.390	-0.1242	0.4394
		1981-2000	-0.01439	0.10594	0.991	-0.2747	0.2460
	1965-1980	1946-1964	-0.15757	0.11466	0.390	-0.4394	0.1242
		1981-2000	-0.17196	0.07508	0.074	-0.3565	0.0126
	1981-2000	1946-1964	0.01439	0.10594	0.991	-0.2460	0.2747
		1965-1980	0.17196	0.07508	0.074	-0.0126	0.3565
Privacy governance reporting	1946-1964	1965-1980	0.06055	0.14283	0.914	-0.2905	0.4116
		1981-2000	-0.11667	0.13197	0.677	-0.4410	0.2077
	1965-1980	1946-1964	-0.06055	0.14283	0.914	-0.4116	0.2905
		1981-2000	-0.17722	0.09353	0.168	-0.4071	0.0526
	1981-2000	1946-1964	0.11667	0.13197	0.677	-0.2077	0.4410
		1965-1980	0.17722	0.09353	0.168	-0.0526	0.4071
Organisational commitment	1946-1964	1965-1980	0.12487	0.12688	0.617	-0.1870	0.4367
		1981-2000	-0.00526	0.11723	0.999	-0.2934	0.2828
	1965-1980	1946-1964	-0.12487	0.12688	0.617	-0.4367	0.1870
		1981-2000	-0.13013	0.08308	0.294	-0.3343	0.0741
	1981-2000	1946-1964	0.00526	0.11723	0.999	-0.2828	0.2934
		1965-1980	0.13013	0.08308	0.294	-0.0741	0.3343

*. The mean difference is significant at the 0.05 level.

Post Hoc Tests – Job level group

Multiple Comparisons

Scheffé

Dependent Variable			Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
						Lower Bound	Upper Bound
Privacy controls assessment	Administrative	Operational	0.02507	0.08639	0.994	-0.2175	0.2677
		Team leader	0.19717	0.13697	0.558	-0.1875	0.5819
		Line /Senior / Exec manager	0.20129	0.12632	0.469	-0.1535	0.5561
	Operational	Administrative	-0.02507	0.08639	0.994	-0.2677	0.2175
		Team leader	0.17209	0.12697	0.607	-0.1845	0.5287
		Line /Senior / Exec manager	0.17622	0.11540	0.507	-0.1479	0.5003
	Team leader	Administrative	-0.19717	0.13697	0.558	-0.5819	0.1875
		Operational	-0.17209	0.12697	0.607	-0.5287	0.1845
		Line /Senior / Exec manager	0.00412	0.15690	1.000	-0.4365	0.4448
	Line /Senior / Exec manager	Administrative	-0.20129	0.12632	0.469	-0.5561	0.1535
		Operational	-0.17622	0.11540	0.507	-0.5003	0.1479
		Team leader	-0.00412	0.15690	1.000	-0.4448	0.4365
Personal information awareness assessment	Administrative	Operational	-0.05233	0.08057	0.936	-0.2786	0.1739
		Team leader	0.01291	0.12775	1.000	-0.3459	0.3717
		Line /Senior / Exec manager	-0.00860	0.11782	1.000	-0.3395	0.3223
	Operational	Administrative	0.05233	0.08057	0.936	-0.1739	0.2786
		Team leader	0.06524	0.11842	0.959	-0.2673	0.3978
		Line /Senior / Exec manager	0.04373	0.10763	0.983	-0.2585	0.3460
	Team leader	Administrative	-0.01291	0.12775	1.000	-0.3717	0.3459
		Operational	-0.06524	0.11842	0.959	-0.3978	0.2673
		Line /Senior / Exec manager	-0.02151	0.14633	0.999	-0.4325	0.3895
	Line /Senior / Exec manager	Administrative	0.00860	0.11782	1.000	-0.3223	0.3395
		Operational	-0.04373	0.10763	0.983	-0.3460	0.2585
		Team leader	0.02151	0.14633	0.999	-0.3895	0.4325
Privacy governance reporting	Administrative	Operational	0.04212	0.10013	0.981	-0.2391	0.3233
		Team leader	0.20436	0.15876	0.647	-0.2415	0.6502
		Line /Senior / Exec manager	0.15609	0.14641	0.768	-0.2551	0.5673
	Operational	Administrative	-0.04212	0.10013	0.981	-0.3233	0.2391

		Team leader	0.16224	0.14717	0.749	-0.2511	0.5755
		Line /Senior / Exec manager	0.11397	0.13376	0.867	-0.2617	0.4896
	Team leader	Administrative	-0.20436	0.15876	0.647	-0.6502	0.2415
		Operational	-0.16224	0.14717	0.749	-0.5755	0.2511
		Line /Senior / Exec manager	-0.04827	0.18185	0.995	-0.5590	0.4624
	Line /Senior / Exec manager	Administrative	-0.15609	0.14641	0.768	-0.5673	0.2551
		Operational	-0.11397	0.13376	0.867	-0.4896	0.2617
		Team leader	0.04827	0.18185	0.995	-0.4624	0.5590
Organisational commitment	Administrative	Operational	-0.01913	0.08902	0.997	-0.2691	0.2309
		Team leader	0.02655	0.14114	0.998	-0.3698	0.4229
		Line /Senior / Exec manager	-0.04993	0.13017	0.986	-0.4155	0.3156
	Operational	Administrative	0.01913	0.08902	0.997	-0.2309	0.2691
		Team leader	0.04567	0.13084	0.989	-0.3218	0.4131
		Line /Senior / Exec manager	-0.03080	0.11891	0.995	-0.3648	0.3032
	Team leader	Administrative	-0.02655	0.14114	0.998	-0.4229	0.3698
		Operational	-0.04567	0.13084	0.989	-0.4131	0.3218
		Line /Senior / Exec manager	-0.07648	0.16167	0.974	-0.5305	0.3776
	Line /Senior / Exec manager	Administrative	0.04993	0.13017	0.986	-0.3156	0.4155
		Operational	0.03080	0.11891	0.995	-0.3032	0.3648
		Team leader	0.07648	0.16167	0.974	-0.3776	0.5305

Post Hoc Tests - Business units

Multiple Comparisons

Scheffé

Dependent Variable			Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
						Lower Bound	Upper Bound
Privacy controls assessment	Insurance / Investment banking	IT	0.03062	0.16054	1.000	-0.4666	0.5278
		Finance / HR / Marketing / Communication	-0.14368	0.20244	0.973	-0.7706	0.4832
		Operations	-0.21849	0.19945	0.878	-0.8362	0.3992
		Retail / Business banking	-0.21058	0.17546	0.837	-0.7540	0.3328
	IT	Insurance / Investment banking	-0.03062	0.16054	1.000	-0.5278	0.4666
		Finance / HR / Marketing / Communication	-0.17430	0.14025	0.819	-0.6086	0.2600
		Operations	-0.24911	0.13590	0.500	-0.6700	0.1717
		Retail / Business banking	-0.24120	0.09734	0.192	-0.5427	0.0603
	Finance / HR / Marketing / Communication	Insurance / Investment banking	0.14368	0.20244	0.973	-0.4832	0.7706
		IT	0.17430	0.14025	0.819	-0.2600	0.6086
		Operations	-0.07481	0.18351	0.997	-0.6431	0.4935
		Retail / Business banking	-0.06690	0.15711	0.996	-0.5534	0.4196
	Operations	Insurance / Investment banking	0.21849	0.19945	0.878	-0.3992	0.8362
		IT	0.24911	0.13590	0.500	-0.1717	0.6700
		Finance / HR / Marketing / Communication	0.07481	0.18351	0.997	-0.4935	0.6431
		Retail / Business banking	0.00791	0.15323	1.000	-0.4666	0.4824
	Retail / Business banking	Insurance / Investment banking	0.21058	0.17546	0.837	-0.3328	0.7540
		IT	0.24120	0.09734	0.192	-0.0603	0.5427
		Finance / HR / Marketing / Communication	0.06690	0.15711	0.996	-0.4196	0.5534
		Operations	-0.00791	0.15323	1.000	-0.4824	0.4666
Personal information awareness assessment	Insurance / Investment banking	IT	-0.11314	0.14471	0.962	-0.5613	0.3350
		Finance / HR / Marketing / Communication	-0.29325	0.18247	0.630	-0.8583	0.2718
		Operations	-0.22237	0.17977	0.821	-0.7791	0.3344
		Retail / Business banking	-0.23718	0.15815	0.690	-0.7270	0.2526
	IT	Insurance / Investment banking	0.11314	0.14471	0.962	-0.3350	0.5613
		Finance / HR / Marketing / Communication	-0.18011	0.12642	0.730	-0.5716	0.2114
		Operations	-0.10923	0.12249	0.939	-0.4886	0.2701

		Retail / Business banking	-0.12404	0.08774	0.736	-0.3958	0.1477
	Finance / HR / Marketing / Communication	Insurance / Investment banking	0.29325	0.18247	0.630	-0.2718	0.8583
		IT	0.18011	0.12642	0.730	-0.2114	0.5716
		Operations	0.07088	0.16541	0.996	-0.4414	0.5831
		Retail / Business banking	0.05607	0.14161	0.997	-0.3825	0.4946
	Operations	Insurance / Investment banking	0.22237	0.17977	0.821	-0.3344	0.7791
		IT	0.10923	0.12249	0.939	-0.2701	0.4886
		Finance / HR / Marketing / Communication	-0.07088	0.16541	0.996	-0.5831	0.4414
		Retail / Business banking	-0.01481	0.13812	1.000	-0.4425	0.4129
	Retail / Business banking	Insurance / Investment banking	0.23718	0.15815	0.690	-0.2526	0.7270
		IT	0.12404	0.08774	0.736	-0.1477	0.3958
		Finance / HR / Marketing / Communication	-0.05607	0.14161	0.997	-0.4946	0.3825
		Operations	0.01481	0.13812	1.000	-0.4129	0.4425
Privacy governance reporting	Insurance / Investment banking	IT	-0.12320	0.18065	0.977	-0.6826	0.4362
		Finance / HR / Marketing / Communication	-0.26599	0.22779	0.850	-0.9714	0.4394
		Operations	-0.37603	0.22442	0.591	-1.0710	0.3190
		Retail / Business banking	-0.27987	0.19743	0.734	-0.8913	0.3315
	IT	Insurance / Investment banking	0.12320	0.18065	0.977	-0.4362	0.6826
		Finance / HR / Marketing / Communication	-0.14279	0.15781	0.936	-0.6315	0.3459
		Operations	-0.25284	0.15291	0.604	-0.7264	0.2207
		Retail / Business banking	-0.15667	0.10953	0.727	-0.4959	0.1825
	Finance / HR / Marketing / Communication	Insurance / Investment banking	0.26599	0.22779	0.850	-0.4394	0.9714
		IT	0.14279	0.15781	0.936	-0.3459	0.6315
		Operations	-0.11005	0.20649	0.991	-0.7495	0.5294
		Retail / Business banking	-0.01388	0.17678	1.000	-0.5614	0.5336
	Operations	Insurance / Investment banking	0.37603	0.22442	0.591	-0.3190	1.0710
		IT	0.25284	0.15291	0.604	-0.2207	0.7264
		Finance / HR / Marketing / Communication	0.11005	0.20649	0.991	-0.5294	0.7495
		Retail / Business banking	0.09616	0.17242	0.989	-0.4378	0.6301
	Retail / Business banking	Insurance / Investment banking	0.27987	0.19743	0.734	-0.3315	0.8913
		IT	0.15667	0.10953	0.727	-0.1825	0.4959

		Finance / HR / Marketing / Communication	0.01388	0.17678	1.000	-0.5336	0.5614
		Operations	-0.09616	0.17242	0.989	-0.6301	0.4378
Organisational commitment	Insurance / Investment banking	IT	-0.00554	0.16056	1.000	-0.5028	0.4917
		Finance / HR / Marketing / Communication	-0.15262	0.20246	0.966	-0.7796	0.4744
		Operations	-0.26001	0.19947	0.791	-0.8778	0.3577
		Retail / Business banking	-0.14455	0.17548	0.954	-0.6880	0.3989
	IT	Insurance / Investment banking	0.00554	0.16056	1.000	-0.4917	0.5028
		Finance / HR / Marketing / Communication	-0.14709	0.14027	0.894	-0.5815	0.2873
		Operations	-0.25447	0.13591	0.478	-0.6754	0.1664
		Retail / Business banking	-0.13902	0.09735	0.729	-0.4405	0.1625
	Finance / HR / Marketing / Communication	Insurance / Investment banking	0.15262	0.20246	0.966	-0.4744	0.7796
		IT	0.14709	0.14027	0.894	-0.2873	0.5815
		Operations	-0.10739	0.18353	0.987	-0.6758	0.4610
		Retail / Business banking	0.00807	0.15713	1.000	-0.4785	0.4947
	Operations	Insurance / Investment banking	0.26001	0.19947	0.791	-0.3577	0.8778
		IT	0.25447	0.13591	0.478	-0.1664	0.6754
		Finance / HR / Marketing / Communication	0.10739	0.18353	0.987	-0.4610	0.6758
		Retail / Business banking	0.11546	0.15325	0.966	-0.3591	0.5901
	Retail / Business banking	Insurance / Investment banking	0.14455	0.17548	0.954	-0.3989	0.6880
		IT	0.13902	0.09735	0.729	-0.1625	0.4405
		Finance / HR / Marketing / Communication	-0.00807	0.15713	1.000	-0.4947	0.4785
		Operations	-0.11546	0.15325	0.966	-0.5901	0.3591

Post Hoc Tests – Length of service group

Multiple Comparisons

Scheffé

Dependent Variable			Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
						Lower Bound	Upper Bound
Privacy controls assessment	1-3 years	4-6 years	0.11340	0.09378	0.691	-0.1500	0.3768
		7-9 years	0.31522	0.14821	0.212	-0.1010	0.7315
		10+ years	0.24053	0.08635	0.053	-0.0020	0.4830
	4-6 years	1-3 years	-0.11340	0.09378	0.691	-0.3768	0.1500
		7-9 years	0.20182	0.15247	0.626	-0.2264	0.6300
		10+ years	0.12713	0.09346	0.605	-0.1354	0.3896
	7-9 years	1-3 years	-0.31522	0.14821	0.212	-0.7315	0.1010
		4-6 years	-0.20182	0.15247	0.626	-0.6300	0.2264
		10+ years	-0.07470	0.14802	0.968	-0.4904	0.3410
	10+ years	1-3 years	-0.24053	0.08635	0.053	-0.4830	0.0020
		4-6 years	-0.12713	0.09346	0.605	-0.3896	0.1354
		7-9 years	0.07470	0.14802	0.968	-0.3410	0.4904
Personal information awareness assessment	1-3 years	4-6 years	0.10043	0.08759	0.726	-0.1455	0.3464
		7-9 years	0.23412	0.13843	0.415	-0.1546	0.6229
		10+ years	0.15626	0.08065	0.291	-0.0702	0.3827
	4-6 years	1-3 years	-0.10043	0.08759	0.726	-0.3464	0.1455
		7-9 years	0.13369	0.14240	0.830	-0.2662	0.5336
		10+ years	0.05583	0.08729	0.938	-0.1893	0.3010
	7-9 years	1-3 years	-0.23412	0.13843	0.415	-0.6229	0.1546
		4-6 years	-0.13369	0.14240	0.830	-0.5336	0.2662
		10+ years	-0.07787	0.13824	0.957	-0.4661	0.3104
	10+ years	1-3 years	-0.15626	0.08065	0.291	-0.3827	0.0702
		4-6 years	-0.05583	0.08729	0.938	-0.3010	0.1893
		7-9 years	0.07787	0.13824	0.957	-0.3104	0.4661
Privacy governance reporting	1-3 years	4-6 years	0.14818	0.10875	0.603	-0.1572	0.4536
		7-9 years	0.35311	0.17187	0.240	-0.1296	0.8358
		10+ years	0.23088	0.10013	0.152	-0.0503	0.5121
	4-6 years	1-3 years	-0.14818	0.10875	0.603	-0.4536	0.1572
		7-9 years	0.20494	0.17680	0.719	-0.2916	0.7015
		10+ years	0.08270	0.10838	0.900	-0.2217	0.3871
	7-9 years	1-3 years	-0.35311	0.17187	0.240	-0.8358	0.1296
		4-6 years	-0.20494	0.17680	0.719	-0.7015	0.2916
		10+ years	-0.12224	0.17164	0.917	-0.6043	0.3598
	10+ years	1-3 years	-0.23088	0.10013	0.152	-0.5121	0.0503

		4-6 years	-0.08270	0.10838	0.900	-0.3871	0.2217
		7-9 years	0.12224	0.17164	0.917	-0.3598	0.6043
Organisational commitment	1-3 years	4-6 years	0.13559	0.09649	0.578	-0.1354	0.4066
		7-9 years	0.29068	0.15250	0.305	-0.1376	0.7190
		10+ years	0.20740	0.08885	0.144	-0.0421	0.4569
	4-6 years	1-3 years	-0.13559	0.09649	0.578	-0.4066	0.1354
		7-9 years	0.15510	0.15688	0.807	-0.2855	0.5957
		10+ years	0.07181	0.09617	0.906	-0.1983	0.3419
	7-9 years	1-3 years	-0.29068	0.15250	0.305	-0.7190	0.1376
		4-6 years	-0.15510	0.15688	0.807	-0.5957	0.2855
		10+ years	-0.08328	0.15230	0.960	-0.5110	0.3444
	10+ years	1-3 years	-0.20740	0.08885	0.144	-0.4569	0.0421
		4-6 years	-0.07181	0.09617	0.906	-0.3419	0.1983
		7-9 years	0.08328	0.15230	0.960	-0.3444	0.5110

Appendix I: Communalities

Communalities

	Initial	Extraction
Q15_S1: 15. My organisation is committed to the protection of personal information.	1.000	0.801
Q16_S1: 16. Management provides me with adequate guidance to implement the regulatory requirements of the Protection of Personal Information Act (POPIA) in my daily duties.	1.000	0.651
Q17_S1: 17. I believe that my organisation effectively governs the protection of personal information with which we work.	1.000	0.757
Q18_S1: 18. Management leads by example to protect personal information.	1.000	0.644
Q19_S1: 19. I believe that my organisation is effective in ensuring that the staff complies with POPIA requirements.	1.000	0.633
Q20_S1: 20. We are encouraged to obtain input from the Information Officer for important business decisions.	1.000	0.627
Q21_S1: 21. I believe that my organisation is effective in implementing the necessary privacy controls.	1.000	0.802
Q22_S1: 22. I believe that my organisation continuously improves the privacy controls.	1.000	0.751
Q23_S1: 23. My organisation has a strong privacy culture.	1.000	0.795
Q24_S1: 24. My organisation ensures that personal information is protected in all our applications.	1.000	0.805
Q25_S1: 25. My organisation effectively ensures that personal information is protected in all our processes.	1.000	0.852
Q26_S1: 26. I have received clear communication from my organisation regarding privacy requirements (e.g. how to protect customer data).	1.000	0.737
Q27_S1: 27. I am aware of the role of the Privacy Office.	1.000	0.734
Q28_S1: 28. My organisation effectively informs us about privacy issues.	1.000	0.755
Q29_S1: 29. My organisation clearly informs us about the responsibility and accountability roles for privacy.	1.000	0.846
Q30_S1: 30. The reporting structures for privacy are clear in my organisation.	1.000	0.841
Q31_S1: 31. I am aware of the timeframe to report a personal data compromise (privacy breach).	1.000	0.787
Q32_S1: 32. All of us know what our responsibilities are for the protection of personal information.	1.000	0.604
Q33_S1: 33. The privacy policy is understandable.	1.000	0.719
Q34_S1: 34. The privacy statement on my organisation's website is understandable.	1.000	0.748
Q35_S1: 35. The privacy policy guides me in the implementation of privacy processes in my daily duties.	1.000	0.746
Q36_S1: 36. The privacy principles (e.g. accountability, openness, security safeguards and information quality) I follow in my daily duties are clearly defined in the privacy policies.	1.000	0.770
Q37_S1: 37. I believe that the business processes and procedures are aligned with the privacy policy.	1.000	0.798
Q38_S1: 38. There are clear privacy standards and procedures in my organisation (e.g. use, disclosure and safeguarding of personal information).	1.000	0.838
Q39_S1: 39. I know how to identify personal information.	1.000	0.802

Q40_S1: 40. I know how to identify special (sensitive) personal information.	1.000	0.805
Q41_S1: 41. My organisation only collects personal information for defined purposes.	1.000	0.715
Q42_S1: 42. I am aware of the business need to collect and process personal information.	1.000	0.807
Q43_S1: 43. My organisation effectively deals with privacy breaches or incidents.	1.000	0.710
Q44_S1: 44. I am aware of the incident management procedure in my organisation to report a privacy incident (e.g. a misdirected email containing personal information).	1.000	0.788
Q45_S1: 45. My organisation clearly communicates what procedure we must follow in the event of a data breach.	1.000	0.760
Q46_S1: 46. I am aware of the consequences of the violation of privacy policies and procedures.	1.000	0.762
Q47_S1: 47. I am aware of the escalation process in my organisation to report a privacy incident.	1.000	0.746
Q48_S1: 48. I am aware of the timeframe to report a personal data compromise (privacy breach).	1.000	0.815
Q49_S1: 49. I am aware of the harmful effects (e.g. on my organisation's brand and reputational damage, loss of market share and revenue, customer distrust or legal action against the company) of the violation of privacy policies and procedures.	1.000	0.748
Q50_S1: 50. I am confident that a contract is in place between my organisation and all service providers.	1.000	0.736
Q51_S1: 51. Service providers are required to adhere to the privacy requirements in their contracts with my organisation.	1.000	0.704
Q52_S1: 52. I am confident that my organisation ensures that service providers protect customers' personal information.	1.000	0.743
Q53_S1: 53. I am confident that my organisation ensures that service providers (e.g. third parties, external consultants and contractors) receive training to protect customers' personal information.	1.000	0.738
Q54_S1: 54. My organisation informs me about my privacy rights.	1.000	0.761
Q55_S1: 55. My organisation has communicated the purpose for collecting customers' personal information.	1.000	0.734
Q56_S1: 56. My organisation will notify me if my personal information has been compromised.	1.000	0.752
Q57_S1: 57. My organisation informs us when there are changes in processes to protect personal information.	1.000	0.820
Q58_S1: 58. The communications that my organisation sends out about the protection of information are always understandable.	1.000	0.792
Q59_S1: 59. Newly appointed colleagues are provided with privacy training.	1.000	0.717
Q60_S1: 60. Privacy training is customised for my job role.	1.000	0.650
Q61_S1: 61. The privacy training equips me to adhere to the privacy policy.	1.000	0.757
Q62_S1: 62. My organisation expects me to complete an annual privacy compliance test.	1.000	0.651
Q63_S1: 63. The privacy training helps me to understand how to protect personal information.	1.000	0.752
Q64_S1: 64. I am confident that my organisation effectively implements measures to identify privacy risks.	1.000	0.847

Q65_S1: 65. I am confident that new processes or systems are assessed for any potential privacy risk (e.g. new application, remote account opening and online applications).	1.000	0.835
Q66_S1: 66. I believe that my organisation is effective in managing privacy risks.	1.000	0.822
Q67_S1: 67. I am confident that my organisation effectively conducts reviews (e.g. internal audits, external audits, and self-assessment) to monitor compliance with its privacy policies and procedures.	1.000	0.819
Q68_S1: 68. I am confident that my organisation effectively monitors compliance with its privacy policies and procedures.	1.000	0.848
Q69_S1: 69. I am confident that my organisation improves the protection of personal information if a weakness is identified.	1.000	0.809
Q70_S1: 70. I believe that the privacy self-assessments adequately prepare my department to be privacy compliant.	1.000	0.804
Q71_S1: 71. I believe that the privacy office effectively prepares my division for privacy audits.	1.000	0.814
Q72_S1: 72. I am confident that my organisation ensures that its privacy policies are aligned with the latest technological advancements.	1.000	0.789
Q73_S1: 73. I am confident that my organisation's privacy controls (e.g. secure print, end-point protection, disk encryption) are effective to protect personal information.	1.000	0.839
Q74_S1: 74. My business unit regularly receives privacy practice updates.	1.000	0.715

Extraction Method: Principal Component Analysis.

Appendix J: Reliability statistics

Scale: Privacy controls assessment

Case Processing Summary

		N	%
Cases	Valid	290	76.9
	Excluded[a]	87	23.1
	Total	377	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardised Items	No. of Items
0.984	0.984	26

Summary Item Statistics

	Mean	Minimum	Maximum	Range	Maximum / Minimum	Variance	No. of Items
Inter-Item Correlations	0.705	0.503	0.879	0.376	1.747	0.004	26

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted
Q67_S167Iamconfidentthatmyorganisationeffectivelyconductsrev Q67_S1: 67. I am confident that my organisation effectively conducts reviews (e.g. internal audits, external audits, and self-assessment) to monitor compliance with its privacy policies and procedures.	103.45	327.162	0.852		0.983
Q68_S168Iamconfidentthatmyorganisationeffectivelymonitorscom Q68_S1: 68. I am confident that my organisation effectively monitors compliance with its privacy policies and procedures.	103.47	325.433	0.869		0.983
Q72_S172Iamconfidentthatmyorganisationensuresthatitsprivacyp Q72_S1: 72. I am confident that my organisation ensures that its privacy policies are aligned with the latest technological advancements.	103.50	322.825	0.855		0.983

Q74_S174Mybusinessunitregularlyreceivesprivacypracticeupdate Q74_S1: 74. My business unit regularly receives privacy practice updates.	103.65	322.788	0.805		0.983
Q71_S171Ibelievethattheprivacyofficeeffectivelypreparesmydiv Q71_S1: 71. I believe that the privacy office effectively prepares my division for privacy audits.	103.55	322.497	0.873		0.983
Q69_S169Iamconfidentthatmyorganisationimprovestheprotectiono Q69_S1: 69. I am confident that my organisation improves the protection of personal information if a weakness is identified.	103.42	327.505	0.819		0.983
Q70_S170Ibelievethattheprivacyselfassessmentsadequatelyprep Q70_S1: 70. I believe that the privacy self-assessments adequately prepare my department to be privacy compliant.	103.49	324.486	0.871		0.983
Q73_S173Iamconfidentthatmyorganisationsprivacycontrolsegse Q73_S1: 73. I am confident that my organisation's privacy controls (e.g. secure print, end-point protection, disk encryption) are effective to protect personal information.	103.49	324.562	0.845		0.983
Q65_S165Iamconfidentthatnewprocessesorsystemsareassessedfora Q65_S1: 65. I am confident that new processes or systems are assessed for any potential privacy risk (e.g. new application, remote account opening and online applications).	103.50	325.573	0.875		0.983
Q53_S153Iamconfidentthatmyorganisationensuresthatserviceprov Q53_S1: 53. I am confident that my organisation ensures that service providers (e.g. third parties, external consultants and contractors) receive training to protect customers' personal information.	103.59	323.807	0.834		0.983
Q56_S156Myorganisationwillnotifymeifmypersonalinformationhas Q56_S1: 56. My organisation will notify me if my personal information has been compromised.	103.68	321.726	0.809		0.983
Q59_S159Newlyappointedcolleaguesareprovidedwithprivacytraini Q59_S1: 59. Newly appointed colleagues are provided with privacy training.	103.53	326.250	0.758		0.983
Q64_S164Iamconfidentthatmyorganisationeffectivelyimplementsm Q64_S1: 64. I am confident that my organisation effectively implements measures to identify privacy risks.	103.48	324.015	0.893		0.983
Q66_S166Ibelievethatmyorganisationiseffectiveinmanagingpriva Q66_S1: 66. I believe that my organisation is effective in managing privacy risks.	103.42	326.342	0.847		0.983

Q50_S150Iamconfidentthatacontractisinplacebetweenmyorganisat Q50_S1: 50. I am confident that a contract is in place between my organisation and all service providers.	103.52	324.063	0.838		0.983
Q57_S157Myorganisationinformsuswhentherearechangesinprocesse Q57_S1: 57. My organisation informs us when there are changes in processes to protect personal information.	103.56	322.275	0.874		0.983
Q54_S154Myorganisationinformsmeaboutmyprivacyrights Q54_S1: 54. My organisation informs me about my privacy rights.	103.58	323.850	0.819		0.983
Q60_S160Privacytrainingiscustomisedformyjobrole Q60_S1: 60. Privacy training is customised for my job role.	103.77	324.370	0.714		0.984
Q58_S158Thecommunicationsthatmyorganisationsendoutaboutthepr Q58_S1: 58. The communications that my organisation sends out about the protection of information are always understandable.	103.54	323.211	0.860		0.983
Q52_S152Iamconfidentthatmyorganisationensuresthatserviceprov Q52_S1: 52. I am confident that my organisation ensures that service providers protect customers' personal information.	103.51	323.988	0.855		0.983
Q37_S137Ibelievethatthebusinessprocessesandproceduresarealig Q37_S1: 37. I believe that the business processes and procedures are aligned with the privacy policy.	103.53	324.146	0.869		0.983
Q61_S161Theprivacytrainingequipsmetoadheretotheprivacypolicy Q61_S1: 61. The privacy training equips me to adhere to the privacy policy.	103.52	326.098	0.817		0.983
Q55_S155Myorganisationhascommunicatedthepurposeforcollecting Q55_S1: 55. My organisation has communicated the purpose for collecting customers' personal information.	103.50	326.417	0.829		0.983
Q43_S143Myorganisationeffectivelydealswithprivacybreachesori Q43_S1: 43. My organisation effectively deals with privacy breaches or incidents.	103.52	326.832	0.771		0.983
Q28_S128Myorganisationeffectivelyinformsusaboutprivacyissues Q28_S1: 28. My organisation effectively informs us about privacy issues.	103.57	321.124	0.823		0.983
Q47_S147Iamawareoftheescalationprocessinmyorganisationtorepo Q47_S1: 47. I am aware of the escalation process in my organisation to report a privacy incident.	103.54	325.038	0.779		0.983

Scale: Personal Information Awareness and Assessment

Case Processing Summary

		N	%
Cases	Valid	354	93.9
	Excluded[a]	23	6.1
	Total	377	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardised Items	No. of Items
0.947	0.947	8

Summary Item Statistics

	Mean	Minimum	Maximum	Range	Maximum / Minimum	Variance	No. of Items
Inter-Item Correlations	0.692	0.571	0.886	0.315	1.552	0.004	8

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted
Q39_S139Iknowhowtoidentifypersonalinformation Q39_S1: 39. I know how to identify personal information.	29.66	21.317	0.836	0.819	0.938
Q40_S140Iknowhowtoidentifyspecialsensitivepersonalinformat Q40_S1: 40. I know how to identify special (sensitive) personal information.	29.68	21.069	0.824	0.809	0.938
Q42_S142Iamawareofthebusinessneedtocollectandprocesspersonal Q42_S1: 42. I am aware of the business need to collect and process personal information.	29.79	20.587	0.857	0.774	0.936
Q41_S141Myorganisationonlycollectspersonalinformationfordefi Q41_S1: 41. My organisation only collects personal information for defined purposes.	29.90	20.343	0.787	0.688	0.941
Q44_S144Iamawareoftheincidentmanagementprocedureinmyorganisa Q44_S1: 44. I am aware of the incident management procedure in my organisation to report a privacy incident (e.g. a misdirected email containing personal information).	29.88	21.050	0.786	0.644	0.941
Q46_S146Iamawareoftheconsequencesoftheviolationofprivacypoli Q46_S1: 46. I am aware of the consequences of the violation of privacy policies and procedures.	29.74	20.936	0.812	0.693	0.939
Q49_S149Iamawareoftheharmfuleffectsegmyorganisationsbranda Q49_S1: 49. I am aware of the harmful effects (e.g. on my organisation's brand and reputational damage, loss of market share and revenue, customer distrust or legal action against the company) of the violation of privacy policies and procedures.	29.69	21.280	0.813	0.690	0.939
Q51_S151Serviceprovidersarerequiredtoadheretotheprivacyrequi Q51_S1: 51. Service providers are required to adhere to the privacy requirements in their contracts with my organisation.	29.77	21.769	0.738	0.591	0.944

Scale: Privacy Governance Reporting

Case Processing Summary

		N	%
Cases	Valid	354	93.9
	Excluded[a]	23	6.1
	Total	377	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardised Items	No. of Items
0.940	0.942	6

Summary Item Statistics

	Mean	Minimum	Maximum	Range	Maximum / Minimum	Variance	No. of Items
Inter-Item Correlations	0.730	0.662	0.799	0.137	1.206	0.002	6

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted
Q27_S127IamawareoftheroleofthePrivacyOffice Q27_S1: 27. I am aware of the role of the Privacy Office.	20.32	15.970	0.776	0.605	0.936
Q29_S129Myorganisationclearlyinformsusabouttherespo nsibility Q29_S1: 29. My organisation clearly informs us about the responsibility and accountability roles for privacy.	20.16	16.468	0.848	0.731	0.927
Q30_S130Thereportingstructuresforprivacyareclearinmy organisa Q30_S1: 30. The reporting structures for privacy are clear in my organisation.	20.32	15.449	0.860	0.748	0.925
Q31_S131Iamawareofthetimeframetoreportapersonaldat acompromis Q31_S1: 31. I am aware of the timeframe to report a personal data compromise (privacy breach).	20.30	15.598	0.849	0.735	0.926
Q35_S135Theprivacypolicyguidesmewiththeimplementat ionofpriva Q35_S1: 35. The privacy policy guides me in the implementation of privacy processes in my daily duties.	20.24	17.318	0.780	0.613	0.935
Q48_S148Iamawareofthetimeframetoreportapersonaldat acompromis Q48_S1: 48. I am aware of the timeframe to report a personal data compromise (privacy breach).	20.26	16.438	0.835	0.712	0.928

Scale: Organisational commitment

Case Processing Summary

		N	%
Cases	Valid	350	92.8
	Excluded[a]	27	7.2
	Total	377	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
0.950	0.952	9

Summary Item Statistics

	Mean	Minimum	Maximum	Range	Maximum / Minimum	Variance	N of Items
Inter-Item Correlations	0.690	0.544	0.911	0.367	1.675	0.007	9

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted
Q15_S115Myorganisationiscommittedtotheprotectionofpersonalin Q15_S1: 15. My organisation is committed to the protection of personal information.	33.70	34.533	0.782	0.664	0.946
Q17_S117Ibelievethatmyorganisationeffectivelygovernstheprote Q17_S1: 17. I believe that my organisation effectively governs the protection of personal information with which we work.	33.88	33.412	0.811	0.703	0.944
Q18_S118Managementleadsbyexampletoprotectpersonalinformation Q18_S1: 18. Management leads by example to protect personal information.	34.11	33.023	0.679	0.499	0.953
Q21_S121Ibelievethatmyorganisationiseffectiveinimplementingt Q21_S1: 21. I believe that my organisation is effective in implementing the necessary privacy controls.	34.02	33.120	0.857	0.791	0.942
Q22_S122Ibelievethatmyorganisationcontinuouslyimprovesthepri Q22_S1: 22. I believe that my organisation continuously improves the privacy controls.	34.00	33.550	0.846	0.822	0.942
Q23_S123Myorganisationhasastrongprivacyculture Q23_S1: 23. My organisation has a strong privacy culture.	33.98	32.596	0.855	0.799	0.942
Q24_S124Myorganisationensuresthatpersonalinformationisprotec Q24_S1: 24. My organisation ensures that personal information is protected in all our applications.	33.92	33.237	0.839	0.849	0.943
Q25_S125Myorganisationeffectivelyensuresthatpersonalinformat Q25_S1: 25. My organisation effectively ensures that personal information is protected in all our processes.	33.93	33.239	0.843	0.851	0.942
Q26_S126Ihavereceivedclearcommunicationfrommyorganisationreg Q26_S1: 26. I have received clear communication from my organisation regarding privacy requirements (e.g. how to protect customer data).	33.91	34.458	0.756	0.609	0.947

Appendix K: Conference paper published - ICTAS 2019 – *A conceptual privacy governance framework*

A conceptual privacy governance framework

Paulus Swartz
College of Science, Engineering and Technology
School of Computing
University of South Africa
Email: paulus.swartz@absa.co.za

Adele Da Veiga
College of Science, Engineering and Technology
School of Computing
University of South Africa
Email: dveiga@unisa.ac.za

Nico Martins
College of Economic and Management Sciences
Department of Industrial and Organisational Psychology
University of South Africa
Email: martinsn@mweb.co.za

Abstract — **Owing to the growth of technological advancements and the enactment of comprehensive data privacy legislation, organisations must meet the requirements of privacy laws. Organisations must incorporate the protection of personal information in their strategic planning and govern it across the organisation. The purpose of this paper is to propose a conceptual privacy governance framework. This is done by comparing existing privacy governance frameworks and proposing a consolidated framework that incorporates a comprehensive set of privacy components that can assist management in governing privacy across an organisation. Such a framework can serve as a point of reference to assist organisations in obtaining the support of senior management, establishing clear processes and delegating responsibilities to individuals, utilising existing standards, and establishing monitoring and audit practices. The privacy governance framework can help to reinforce privacy protection, enhance the organisation's reputation, foster a culture of privacy and ensure compliance with privacy regulatory requirements.**

Keywords—***Privacy, privacy governance, privacy governance framework, Protection of Personal Information Act, POPIA***

I. Introduction

Organisations sometimes lose sight of their responsibilities and accountability as stipulated by regulatory laws [1]. Responsible parties (i.e. organisations) process, store, update, delete, modify and collect personal information using technology. According to the Protection of Personal Information Act (POPIA) [2], responsible parties must not only have permission for, but are also held accountable when processing personal information [2]. According to the IAPP-EY survey, privacy awareness is increasing and organisations are accepting accountability for the protection of personal information [3]. Privacy frameworks help management to enforce accountability, to use ongoing compliance monitoring, to establish privacy policies, to develop automated privacy procedures and manuals, and to deliver privacy training [4].

In November 2013, POPIA was signed into law by the President of South Africa. This Act was promulgated to protect the privacy of individuals when personal information is processed by organisations [2]. Data protection legislation across the European Union was harmonised by the European Commission and by the adoption of the EU's Data Directive 95/48/EC [20]. The latter directive has recently been updated and is now called the General Data Protection Regulation (GDPR) [5], which addresses the latest technological developments [6]. A comparison study has been done and results show that POPIA is largely in line with the principles of GDPR and other countries [7].

A 2017 study of the South African market shows that major work needs to be done to facilitate the protection of personal information in organisations [8]. According to the study, only 28.6% of organisations are aware of personal data protection training and awareness programmes, and only 37.5% of the participants have indicated that they are aware of the implications of non-compliance with POPIA [8]. South African organisations require assistance to govern privacy effectively to meet their legal requirements. There is a need for a holistic, all encompassing, privacy governance framework that organisations in South Africa could use as a point of reference to govern the implementation of privacy.

II. Research Objective

The objective of this paper is to develop a conceptual privacy governance framework that might be used by organisations to govern the implementation of privacy requirements and laws, such as POPIA. This is done by reviewing existing privacy governance frameworks to compare their components and to derive a common set of components for completeness. The consolidated components of the existing privacy governance frameworks are integrated to propose a holistic privacy governance framework using the existing theory and research approach of Maxwell [9].

This paper discusses the first phase of the research, which entails the development of a conceptual framework using available literature. The second phase of the research focuses on the development of a validated questionnaire based on the conceptual privacy governance framework; this questionnaire would then be used to measure employees' perception of how well privacy is governed in an organisation. The first phase aims to establish content validity and to evaluate the theoretical perspective(s) driving the privacy governance measuring instrument. During this phase, the use of theory to develop the items of the measuring instrument [10] is also investigated.

ISBN 978-1-5386-7365-2/19/$31.00 ©2019 IEEE

III. BACKGROUND

A. Protection of Personal Information Act 4, 2013 (POPIA)

Sections 1, 112 and 113 and Part A of Chapter 5 of POPIA are currently implemented. These relate to the appointment of an information regulator [13]. POPIA was promulgated to protect the privacy of individuals when personal information is processed by organisations [2]. Organisations, as responsible parties, must ensure that they meet the conditions for the lawful processing of personal information (see Condition 1 of POPIA). The responsible party is therefore responsible for protecting personal information and ensuring the lawful processing of such information.

Organisations have a one-year grace period to comply with POPIA once the President proclaims the commencement date [11]. South African organisations still have time to put policies, procedures and privacy frameworks in place, as POPIA has not been fully implemented as yet [12]. The remaining sections of POPIA will be implemented once the information regulator becomes fully operational [13].

IV. PRIVACY GOVERNANCE

A. Governance

The King III report (2009) states that good governance is about effective leadership. The King IV report has come into effect on 1 April 2017 [14], and focuses on ethical and effective leadership in South Africa [15]. Such leadership is characterised by the ethical values of transparency, fairness, responsibility and accountability, and is based on moral duties [16]. Company strategies and operations are directed by responsible leaders who aim to meet their companies' social and environmental responsibilities, and to ensure sustainable economic performance [16]. Governance therefore contributes to the effectiveness and efficiency of the organisation [17]. There is a strong relationship between good governance and compliance with the law, such as POPIA [16].

B. Privacy governance

According to the Information Systems Audit and Control Association (ISACA), privacy governance means that the directors of an organisation should direct, evaluate and monitor the privacy requirements and vision based on business needs [18]. Privacy governance in an organisation provides direction and strategy, and key privacy issues are discussed and decided upon [19]. It is linked to an organisation's privacy policy, which should govern the protection and processing of personal information [20]. Privacy governance is therefore a strategic approach by management to communicate the core values of the processing and protection of personal information to the stakeholders [21].

A clear accountability policy is a key requirement for good privacy governance; it should spell out who is responsible for the various functions and aspects of the privacy management programme [22]. The benefit of an effective privacy governance framework is that it identifies the personal information available to the business and the processes followed to handle such information. In addition it determines the risks related to the information and stipulates how those the risks can be reduced by implementing controls [34]. Privacy governance frameworks assist in creating responsibilities and the necessary roles to maintain and build a privacy-aware and privacy-ready organisation [21].

V. DEVELOPMENT OF THE CONCEPTUAL PRIVACY GOVERNANCE FRAMEWORK

A privacy programme requires support from senior management, the establishment of clear processes and the delegation of responsibilities to individuals, the utilisation of existing standards, and the establishment of monitoring and audit practices [23]. It is difficult to assess whether all the privacy guidelines or criteria of a privacy programme have been implemented successfully when there is no privacy framework in place [24]. A privacy governance framework clarifies each employee's role in privacy management to ensure that the responsible party is held accountable [26]. Privacy governance frameworks enforce accountability, use ongoing compliance monitoring, establish privacy policies, develop automated privacy procedures and manuals and, lastly, they deliver input for privacy training [4].

A conceptual framework is defined as "either graphically or in narrative form, the main things to be studied – the key factors, constructs or variables – and the presumed relationships among them" [25]. A conceptual framework is primarily a model or conception of what needs to be studied [9], and is something constructed and not merely founded [15]. The conceptual privacy governance framework proposed in this study incorporates components taken from various existing privacy governance frameworks in the literature, which has been analysed critically [9].

In this study, existing theory is used to identify important components that should be included in a conceptual framework for privacy governance. Existing theory sheds light on phenomena and relationships that can be depicted visually to represent the conceptual framework [15]. The most prevalent privacy governance frameworks are discussed and compared in the next section to derive a common set of components for constructing the conceptual privacy governance framework.

A. Privacy governance framework comparison

Four privacy governance frameworks have been selected for the comparison, namely "Information and Privacy Commission of New South Wales: Privacy Governance Framework" (IPC) [26]; "Common Privacy Framework of the Information Privacy Commissioner of Ontario – CCIM Assessment Projects" [19]; "Privacy Management Program – The Office of the Privacy Commissioner of Canada" (OIPC) [27]; and "The Office of the Australian Information Commissioner (OAIC) – Privacy Management Framework" [28].

These frameworks are comprehensive and address the privacy principles implemented by the OECD [12]. The OECD privacy principles comprise the following eight principles: (1) collection limitation; (2) data quality; (3) individual participation; (4) purpose specification; (5) use limitation; (6) security safeguards; (7) openness; and (8) accountability [29]; they also map to the conditions of POPIA. The Privacy Management Program of the Office of the Privacy Commissioner for Personal Data, Hong Kong

(PCPD), has been excluded, because it is modelled on the framework of the OIPC [30], which includes the same key components. The GAPP privacy principles have also been excluded, as the primary objective of the principles is to facilitate privacy compliance and the secondary objective is to focus on privacy auditing [31].The next section is an overview of the four privacy governance frameworks:

1) The *OIPC privacy management framework* has two parts, namely Part A: building blocks (organisational commitment and programme controls); and Part B: ongoing assessment and revision. Organisational commitment consists of: buy-in from the top; privacy officer; privacy office; and reporting. the programme controls consist of the personal information inventory; policies; risk assessment tools; training and education requirements; breach and incident management response protocols; service provider management; and external communication.

2) The *IPC privacy governance framework* consists of five elements, namely: element 1: setting leadership and governance; element 2: planning and strategy; element 3: programme and service delivery; element 4: complaint incident management; and element 5: evaluating and reporting. The IPC privacy governance framework is based on the Privacy and Personal Information Protection Act of 1998 (PPIP Act).

3) The *CCIM common privacy governance framework* consists of three sections, namely: privacy governance; privacy policies and procedures; and privacy operations. The privacy operations section consists of the following subsections: consent management; breach management; awareness and training; client privacy rights support; log review; communication; and privacy operations review.

4) The *OAIC privacy governance framework* consist of four steps, namely: step 1: embed: a culture of privacy that enables compliance; step 2: establish: robust and effective privacy practices, procedures and systems; step 3: evaluate: your privacy practices, procedures and systems to ensure continued effectiveness; and step 4: enhance: your response to privacy issues. These steps of the framework are based on the Australian Privacy Principle (APP), which is contained in the Privacy Act 1988 [32].

A comparison table (Table I) has been drafted to compare the components of the selected privacy governance frameworks. The complete set of components derived from each of the privacy governance frameworks (14 in total) is included in the first column under the heading "Components". In the top row, under "Privacy governance framework", the frameworks that have been discussed are listed. The "x" indicates that a component is listed in the specific privacy governance framework. Each empty space in a specific framework column means that the component is not part of that specific framework. The total column gives an indication of how many of the components each framework has. The OIPC and OAIC privacy frameworks each have 12 of the 14 components listed in column one. The IPC has 11 components, while the CCIM has eight. The OIPC and OAIC frameworks are the most comprehensive frameworks and the CCIM is the least comprehensive framework. All four privacy governance frameworks have seven components (1, 2, 3, 5, 7, 8 and 12) in common. The OAIC is the only framework that has the privacy feedback channel (employees & clients) component.

B. Conceptual framework for privacy governance

The 14 components of the privacy governance frameworks listed in table 1 were grouped into four main categories, namely (a) *Organisational commitment*; (b) *Policies and procedures*; (c) *Privacy programme controls*; and (d) *Ongoing assessment and review*. New names have been given to the 14 components. The oversight and review plan (12) and assess and revise programme controls (13) have been combined in one subcomponent called "Ongoing assessments and evaluation". Both components 12 and 13 in Table I refer to the review and monitoring of the privacy programme controls. Table II gives an overview of how the components of the conceptual privacy governance framework map to the 13 components listed in the privacy governance framework comparison table (see Table I). Component 1 in Table I has been changed to "Leadership commitment", as it addresses the leadership of the organisation. Components 7 and 14 have been combined and are now called "Privacy awareness and training", as it addresses the training of employees and the promotion of privacy awareness.

Component 10 of Table I has been changed to "Service provider management", as it addresses the processing of data

TABLE I.
PRIVACY GOVERNANCE FRAMEWORK COMPARISON TABLE (SOURCE: RESEARCHER)

Components	OIPCs (Canada)	IPC North South Wales	CCIM – Ontario	OAIC – Australia	Total
Buy in from the top	x	x	x	x	4
Data protection officer/office	x	x	x	x	4
Reporting	x	x	x	x	4
Personal data inventory	x			x	2
Policies	x	x	x	x	4
Risk assessment tools	x			x	2
Training and education requirements	x	x	x	x	4
Breach handling/ incident management	x	x	x	x	4
Communication	x	x	x		3
Data processor/ service provider management	x	x			2
Programme assurance/ audit			x	x	2
Oversight and review plan	x	x	x	x	4
Assess and revise programme controls	x	x		x	3
Promote the plan (awareness)		x		x	2
Total (14)	12	11	9	12	

and the handling of personal information by third parties. The numbers in column two, the "Reference to Table I" column, refer to the components in the "Elements" column of Table I. Each component of the conceptual privacy governance framework in the "Elements" column maps to the components that are numbered 1 to 14 in Table I. Table II illustrates that all the components of the existing privacy governance frameworks are incorporated in the conceptual privacy governance framework.

Fig 1 depicts the components of the conceptual privacy governance framework based on the consolidated elements in table II. All the components follow a top–down approach, from management to employees, to implement all the privacy structures, policies and procedures, and thus to ensure the protection of personal information. The next section discusses the conceptual privacy governance framework and its related components.

C. *Components of the conceptual framework for privacy governance*

The conceptual privacy governance framework starts with the *organisational commitment*, which is formulated based on the governing board's privacy objectives and strategy. The *privacy policies and procedures* are then developed by senior managers of the organisation, and are communicated to the privacy programme management section responsible for implementing the *privacy programme controls*. The *ongoing assessment and review* section of the framework focuses on assessing and reviewing the privacy programme controls, and communicating the report to the privacy programme managers and stakeholders of the organisation. The effectiveness of the privacy programme or privacy breaches are reported to the relevant stakeholders. The audit reports are then reviewed by the information officer and the governing body, whereafter they revise the privacy policies and the procedures to ensure that the organisation is compliant with privacy regulations.

The conceptual privacy governance framework is characterised by an ongoing process flow. Its aims are to ensure that the right policies and procedures are communicated to the relevant stakeholders, and to promote a privacy culture among employees. The conceptual privacy governance framework flow begins with the *organisational commitment*, which sets out the privacy strategies and objectives of the organisation, and makes provision for the appointment of a privacy officer and the establishment of a privacy office. From these privacy strategies and objectives, the *policies and procedures* are developed to give guidance to the employees of the organisation. The *privacy programme controls* are then developed to ensure that the policies and procedures are implemented, and that they are compliant with privacy legislation [12]. This is followed by the *ongoing assessment and review* stage of the framework, which focuses on ensuring that the privacy programme controls, policies and procedures are continuously assessed and reviewed to ensure the effectiveness, accountability and compliance of the privacy programme.

At the organisational commitment stage, the assessment and review reports are assessed by senior management and all stakeholders. The privacy policies and the privacy programme controls can then be updated based on their findings. The conceptual privacy governance framework incorporates continuous flow to ensure that all policies are updated to meet the requirements of the latest privacy laws and technological advancements. The privacy programme controls must also be adapted when changes occur to ensure their compliance and effectiveness [12].

Here follows a brief description of each of the subcomponents of the conceptual privacy governance framework:

1) *Leadership commitment*: The leadership of the organisation is responsible for setting the strategic direction

TABLE I. MAPPING OF CONCEPTUAL PRIVACY GOVERNANCE FRAMEWORK COMPONENTS IN TABLE I

Main components	Subcomponents	Reference to Table I
Organisational commitment	Leadership commitment	1
	Information officer	2
	Privacy office	2
	Reporting	3
Privacy policies and procedures	Policies and procedures	5
Privacy programme controls	Personal information inventory	4
	Service provider management	10
	Breach handling/ incident management	8
	Communication	9
	Privacy awareness and training	7, 14
	Risk assessment tools	6
	Programme Assurance / Audit	11
Ongoing assessments and evaluation	Ongoing assessment and review	12, 13

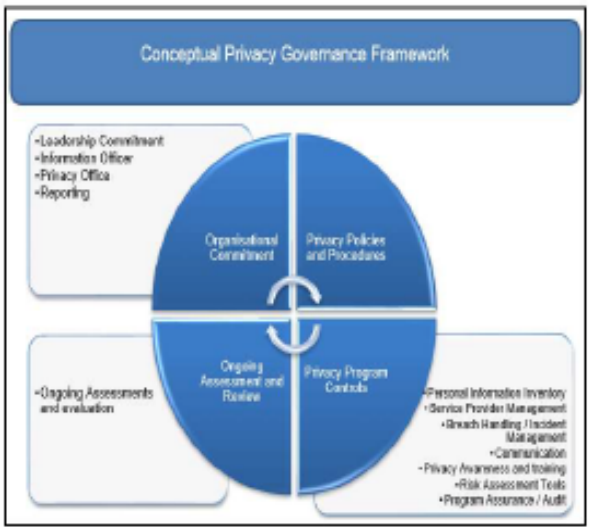


Fig. 1 Conceptual Privacy Governance Framework

for privacy, approving privacy policies, overseeing and monitoring the privacy programme, and ensuring accountability.

2) Information officer: Part B of Chapter 5 (section 55) of POPIA describes the responsibilities of an information officer and a deputy information officer. The role of the information officer is very important for the strategic planning of the business, as well as for the assessment and revision of the privacy programme [33].

3) *Privacy office*: The privacy office team usually consists of different team members from all areas of the organisation [34]. The main responsibilities of the privacy office, as identified by the IAPP-EY privacy governance survey, are the development of privacy policies and procedures; facilitating privacy awareness and training; the management of privacy breaches and incidents; designing and implementing privacy controls; communication; and privacy impact assessment [3].

4) Reporting: Principle 5 of the King IV report states that the reports issued by the governing body of the organisation helps the stakeholders to make informed assessments and demonstrates that the organisation complies with the relevant laws [15].

5) *Policies and procedures*: Policies and operational plans are developed by management to give direction to privacy strategies, according to the King IV report, and must be approved by the governing body [15].

6) *Personal information inventory:* The organisation has to keep an inventory of the personal information records that they process [3]. Organisations must document and understand the personal information it processes and where it is stored [27].

7) *Service provider management:* Third-party agreements and audit procedures must be in place to ensure compliance with the organisation's privacy policies and procedures [35]. The service provider must comply with the service level agreement or contract, which includes adherence to the organisation's privacy policies [33].

8) *Breach handling/incident management*: Privacy breaches and security incidents can occur due to unauthorised access to data, negligence of employees, and malicious and criminal attacks [36]. Breach-handling procedures must be clearly documented and include five activities, namely: detections; escalation; breach handling; breach notification; and reporting [19].

9) *Communication:* Condition 6 of POPIA requires the responsible party to be open and transparent [2]. Organisations have a responsibility to inform the individuals of their privacy rights by means of privacy notices on their websites, social media and mobile communication platforms [33, 11].

10) *Privacy awareness and training*: Privacy training must be conducted annually to assess employees' understanding and to inform employees of any changes to privacy policies and procedures [35].

11) *Risk assessment tools*: Privacy impact assessments can assist organisations in mitigating and identifying security risks and leakages [37]. Risk assessment procedures must be in place to assess, identify and manage the privacy risk [3, 43].

12) *Programme assurance/Audit:* Ensure that internal and external audits are conducted to monitor compliance with the privacy policies. To improve the privacy processes, internal audits need to be conducted to identify areas of improvement [27]. In addition, privacy self-assessments must be conducted by business units [37].

13) *Ongoing assessment and review*: An oversight and review plan must be implemented by the privacy officer to ensure that the privacy management programme is monitored and assessed effectively [27]. The objective of the review plan is to ensure that the privacy operations are executed in line with the defined privacy processes [19]. Privacy controls must be evaluated and updated on a regular basis [3, 43].

VI. FUTURE RESEARCH AND LIMITATIONS

The privacy governance framework is a conceptual framework that has not yet been validated. As part of ongoing research and the conceptual framework will be used to develop questionnaire statements that measure the perceptions of employees about the governance of privacy in an organisation. Future research will focus on validating the questionnaire and framework using statistical analysis.

VII. CONCLUSION

Privacy has a long history and comprehensive data privacy laws now number more than 120 globally. In South Africa, POPIA has not yet been implemented, but an Information Regulator has been established. The research objective was to propose a conceptual privacy governance framework that could assist South African organisations in governing privacy in line with POPIA. This was achieved by comparing existing privacy governance frameworks to derive a common set of privacy components that could be used to compile a conceptual privacy governance framework. The proposed privacy governance framework includes 13 common components that organisations can focus on to govern privacy effectively in the organisation, thereby reinforcing the protection of personal information, fostering a culture of privacy, enhancing the organisational reputation and ensuring privacy compliance. Future research will include the development of a questionnaire based on the proposed framework, which will be validated statistically.

REFERENCES

[1] Ernest and Young, "Privacy trends 2014: Privacy protection in the age of technology," 2014. [Online]. Available: http://www.ey.com/Publication/vwLUAssets/EY_-_Privacy_trends_2014:_Privacy_protection_in_the_age_of_technology/$FILE/EY-Insights-on-GRC-Privacy-trends-2014.pdf. [Accessed: 27-Oct-2016].

[2] POPIA, "Protection Personal information Act, 2013," *Natl. Gazettes, No 37067*, vol. 581, no. 37067, pp. 1–148, 2013.

[3] T. Hughes and S. Leizerov, "IAPP-EY Annual Privacy Governance Report 2016," *IAPP-EY*, 2016. [Online]. Available: https://iapp.org/media/pdf/resource_center/IAPP-2016-GOVERNANCE-SURVEY-FINAL2.pdf. [Accessed: 10-Oct-2016].

[4] D. Pelkola, "A framework for managing privacy-enhancing technology," *IEEE Softw.*, vol. 29, pp. 45–49, 2012.

[5] GDPR, "General Data Protection Regulation (EU) 2016/679," *Official Journal of the European Union*, 2016. [Online]. Available: http://eur-

lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&qid=1490179745294&from=en. [Accessed: 27-Jun-2017].

[6] Allen & Overy, "The EU General Data Protection Regulation is finally agreed," *Allen & Overy*, vol. 1, 2016.

[7] J. Botha, M. M. Grobler, J. Hahn, and M. M. Eloff, "A High-Level Comparison between the South African Protection of Personal Information Act and International Data Protection Laws," *12th Int. Conf. Cyber Warf. Secur.*, vol. 12, pp. 57–66, 2017.

[8] N. Baloyi and P. Kotze, "Are organisations in South Africa ready to comply with personal data protection or privacy legislation and regulations?," *2017 IST-Africa Week Conf. IST-Africa 2017*, pp. 1–11, 2017.

[9] J. A. Maxwell, "Conceptual Framework: What do you think is going on?," in *Qualitative Research Design: An Interactive Approach*, 2013, pp. 39–72.

[10] M. Saunders, P. Lewis, and A. Thornhill, *Research Methods for Business Students*, 7th ed. England: Pearson Education Limited, 2016.

[11] Michalsons, "Protection of Personal Information Act Summary | POPIA,"2017. [Online]. Available: https://www.michalsons.com/focus-areas/privacy-and-data-protection/protection-of-personal-information-act-popia. [Accessed: 08-May-2017].

[12] M. De Bruyn, "The Protection of Personal Information (POPI) Act - Impact on South Africa," *Int. Bus. Econ. Res. J.*, vol. 13, no. 6, pp. 1315–1340, 2014.

[13] Information Regulator of South Africa, "Press briefing by the Information Regulator 20 September 2017," 2017. [Online]. Available: http://www.justice.gov.za/inforeg/docs/ms-20170920-InfoRegBriefing.pdf. [Accessed: 21-Jun-2018].

[14] C. Clamp, "King III vs King IV - What you really need to know," *Grant Thornton South Africa.*, 2017. [Online]. Available: https://www.grantthornton.co.za/globalassets/1.-member-firms/south-africa/pdfs/kingiv_feb17.pdf. [Accessed: 17-Sep-2017].

[15] IODSA, "King IV Report on Corporate Governance for South Africa 2016," *King IV*, 2016. [Online]. Available: http://c.ymcdn.com/sites/www.iodsa.co.za/resource/resmgr/king_iv/King_IV_Report/IoDSA_King_IV_Report_-_WebVe.pdf. [Accessed: 31-Aug-2017].

[16] King III Report, "King Code of Governance for South Africa 2009," *Institute of Directors in Southern Africa*, 2009. [Online]. Available: http://www.ngopulse.org/sites/default/files/king_code_of_governance_for_sa_2009_updated_june_2012.pdf. [Accessed: 18-May-2016].

[17] B. Klievink, N. Bharosa, and Y. H. Tan, "The collaborative realization of public values and business goals: Governance and infrastructure of public-private information platforms," *Gov. Inf. Q.*, vol. 33, no. 1, pp. 67–79, 2016.

[18] M. Vael, "Privacy compliance laws: Why the European Commission has finally got it right," *CSO Online*, 2012. [Online]. Available: http://www.csoonline.com/article/2132708/privacy/privacy-compliance-laws--why-the-european-commission-has-finally-got-it-right.html. [Accessed: 19-Jul-2017].

[19] CCIM, "Common Privacy Framework CCIM Assessment Projects," *Community Care Information Management*, 2010. [Online]. Available: https://www.ccim.on.ca/Documents/CPF/CCIM_CommonPrivacyFramework_v1.0_CPF.pdf. [Accessed: 14-Aug-2016].

[20] M. F. Dennedy, J. Fox, and T. R. Finneran, "Data and privacy governance concepts," in *The Privacy Engineer's Manifesto. Apress*, 2014, pp. 51–72.

[21] M. Dennedy, J. Fox, and T. Finneran, "Developing Privacy Engineering Requirements," *Priv. Eng. Manif.*, pp. 93–119, 2014.

[22] E. Denham, "An examination of BC Government's privacy breach management," *Office of the Information and Privacy Commissioner*, 2015. [Online]. Available: https://www.oipc.bc.ca/media/16876/oipc-examination-of-bc-governments-privacy-breach-management.pdf. [Accessed: 19-Jul-2017].

[23] S. Pearson, "Privacy Management in Global Organisations," *IFIP Int. Fed. Inf. Process.*, pp. 217–237, 2012.

[24] I. Kroener and D. Wright, "A Strategy for Operationalizing Privacy by Design," *Inf. Soc.*, vol. 30, no. 5, pp. 355–365, 2014.

[25] M. B. Miles and A. M. Huberman, "Focusing and bounding the collection of data: The substantive start," in *Qualitative Data Analysis: An Expanded Sourcebook*, 2nd ed., Thousand Oaks, London, and New Delhi: Sage Publication, 1994, pp. 16–38.

[26] T. Pilgrim, "Privacy Governance Framework," *Information and privacy commission NSW*, 2014. [Online]. Available: http://www.ipc.nsw.gov.au/privacy-governance-framework#. [Accessed: 13-Aug-2016].

[27] OIPC, "Getting Accountability Right with a Privacy Management Program," *Office of the Information and Privacy Commissioner*, 2016. [Online]. Available: https://www.oipc.bc.ca/guidance-documents/1435. [Accessed: 10-Oct-2016].

[28] OAIC, "Privacy management framework: enabling compliance and encouraging good practice," *Office of the Australian Information Commissioner Privacy*, 2015. [Online]. Available: https://www.oaic.gov.au/agencies-and-organisations/guides/privacy-management-framework. [Accessed: 25-Jul-2017].

[29] OECD, "The OECD Privacy Framework," 2013. [Online]. Available: http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf. [Accessed: 10-Oct-2016].

[30] PCPD, "Privacy Management Programme: A Best Practice Guide," *Office of the Privacy Commissioner for Personal Data, Hong Kong*, 2014. [Online]. Available: https://www.pcpd.org.hk/pmp/files/PMP_guide_e.pdf. [Accessed: 07-Oct-2017].

[31] AICPA and Chartered Accountants of Canada, "Generally Accepted Privacy Principles," no. August, pp. 1–84, 2009.

[32] Australia Privacy Act, *Privacy Act 1988 No 119*. Australia, 1988, pp. 1–385.

[33] K. M. Herath, *Building a privacy program. A practitioner's guide*. Portsmouth: International Association of Privacy Professionals (IAPP), 2011.

[34] R. Herold, "Building an effective privacy program," *Inf. Syst. Secur.*, vol. 15, no. 3, pp. 24–35, 2006.

[35] AICPA/CICA, "Privacy Maturity Model," *AICPA/CICA*, 2011. [Online]. Available: https://www.kscpa.org/writable/files/AICPADocuments/10-229_aicpa_cica_privacy_maturity_model_finalebook.pdf. [Accessed: 14-Nov-2017].

[36] N. Martins and A. Da Veiga, "Factorial Invariance of an Information Security Culture Assessment Instrument for Multinational Organisations With Operations," *J. Gov. Regul.*, vol. 4, no. 4, pp. 1–13, 2015.

[37] A. Da Veiga and N. Martins, "Information security culture and information protection culture: A validated assessment instrument," *Comput. Law Secur. Rev.*, vol. 31, no. 2, pp. 243–256, 2015.

Appendix L: Declaration by language practitioner

DECLARATION BY LANGUAGE PRACTITIONER

I, Yvonne Smuts, hereby declare that I have been appointed by Paulus Swartz ("the candidate") to attend to the linguistic aspects of the research report that is hereby submitted in partial fulfilment of the requirements for the degree MSc Information Systems in the School of Computing of the University of South Africa.

To the best of my knowledge, all suggestions and recommendations made by me in this regard have been attended to by the candidate.

Title of dissertation: *A validated information privacy governance questionnaire to measure the perception of how effective privacy is governed in a financial institution in the South African context*

Date: .....8 March 2019

(Ms) Y Smuts

BA (Languages) (UP)

HED (cum laude) (UP)

SATI Accredited Translator (1002242)

Member Prolingua